LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvallisuuden hallinnan suunnittelu ja toteutus

Projektimalli ja – opas valtionhallintoon

Nurmi, Kirsi

2011 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Tietoturvallisuuden hallinnan suunnittelu ja toteutus
Projektimalli ja – opas valtionhallintoon

Kirsi Nurmi
Turvallisuusosaamisen koulutus-
ohjelma
Opinnäytetyö
Marraskuu, 2011

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusosaamisen koulutusohjelma
Ylempi ammattikrkeakoulututkinto

Kirsi Nurmi

Tietoturvallisuuden hallinnan suunnittelu ja toteutus
Projektimalli ja – opas valtionhallintoon

Vuosi 2011 Sivumäärä 41 + 65

Tämän kehittämistehtävän tavoitteena oli laatia menetelmä (vaiheistus, tehtävät ja lopputulokset), jonka avulla organisaatio voi kehittää tietoturvallisuutta sellaisina kokonaisuuksina, joissa sitä on aikaisempaa helpompi hallinta projektin avulla. Menetelmän tueksi laadittiin projektiopas, jossa kerrotaan vaiheittain, miten tietoturvallisuuden kehittämishanketta voidaan viedä eteenpäin.

Projektimalli- ja opas laadittiin työelämälähtöisesti, perustuen käytännön kokemukseen ja yhteistyöhön tietoturvallisuuden asiantuntijoiden kanssa. Kehittämistyössä käytettiin suunnittelutieteeseen kuuluva konstruktiivista tutkimusmenetelmää. Toteuttamisvaihe perustui rinnakkaiseen spesifiointi- ja implementointiprosessiin.

Projektimalli ja – oppaan rakenne tukevat tietoturvallisuuden kokonaisuuden hallintaa keräten tietoturvallisuuden politiikat, linjaukset, ohjeistukset sekä käytänteet yhteen. Rakenne mahdollistaa kokonaisuuden laajentamisen ja syventämisen. Kokonaisuuteen voidaan liittää olemassa olevia politiikkoja, linjauksia, ohjeistoa, dokumenttipohjia, työkaluja ja muuta tietoturvallisuuden hallintaa tukevaa materiaalia. Näin asiantuntija löytää kuhunkin tehtävään tukea aikaisempaa helpommin.

Sekä menetelmä, että projektiopas otettiin vaiheittain käyttöön, ensin kuuden valtionhallinnon organisaation yhteishankkeessa. Tämän jälkeen menetelmää sovellettiin valtiovarainministeriössä ja lopuksi se otettiin oppaineen käyttöön laajemmin Valtiovarainministeriön tietoturvallisuusasetuksen toimeenpanohankkeessa (Asettamispäätös VM 047:15/2007). Sekä projektimalli, että projektiopas ovat vapaasti organisaatioiden käytössä ja projektiopas on veloituksetta ladattavissa mm. www.tietoturvatalkoot.fi –sivustolla.

Asiasanat: Projektimalli, projektiopas, tietoturvallisuuden hallinta

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Master´s Degree in Security Management

Kirsi Nurmi

Project Model and Guide for Implementing an Information Security Management System

Year 2011 Pages 41 + 65

The task of this thesis was to create a project model and guide to help with planning and implementing an information security management system. In the project guide it is practically advised how to execute different tasks. The guide was based on a practical experience and co-operation with several information security experts.

In the development work for project model and guide constructive method was used during the development. The project model and guide was based on concurrent processes of specification and implementation.

The project model and the structure of the project guide collect various guides and tools together into pre organized collection. Existing policies, regulations, document models, tools and other materials which support information security management can also be connected to the entity. This way, it is easier to find support for different tasks.

The results of the dissertation were estimated and were utilized at the first stage in the joint venture of six organizations coordinated by the Government IT Shared Service Centre at the State Treasury Finland. After this the project model and guide were used organization-specifically, among others, in the development of the internal information security of ministry of finance.

Key words: Information Security Management, Information security implementation, project model

Sisällys

1 Johdanto

Keväällä 2011 viestintäministeriö Suvi Lindén piti puheen kansallisen tietoturvaviikon yhteydessä järjestetyssä tietoturvatapahtumassa. Hän kertoi puheessaan, että tietoturvallisuudesta on tullut lähes päivittäinen yhteiskunnallinen puheenaihe. Tietoturvallisuuden asema on muuttunut tärkeämmäksi, kun yhteiskunnan tärkeimpiä toimintoja siirretään toimimaan tieto- ja viestintäjärjestelmien varaan. Lindén huomautti, että tietoturvallisuuden perustaso tulee saada normaaleissa arkiolosuhteissa kansainvälisesti verraten korkeimmalle tasolle. Näin voidaan varautua myös niihin tilanteisiin, joissa järjestelmiin kohdistuu erilaisia häiriöitä. (Linden 2011) Lindénin puheesta nousee keskeiseksi käsite ”perustaso”. Tästä herää kysymys: Mitä tarkoittaa perustason saaminen korkeammalle tasolle ja miten tämä tapahtuu?

1.1 Aihepiirin esittely ja tärkeys

Perustason tietoturvavaatimukset on koottu kymmenen kohdan listaksi Asetuksessa tietoturvallisuudesta valtionhallinnossa (TTA 681/2010). Vaatimukset koskevat valtion viranomaisia, eli valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia.

Tietoturvataso ei ole käsitteenä yksiselitteinen. Vuonna 2007 ValtIT:n tietoturvatasojen esitutkimushanke selvitti 20 valtionhallinnon tietoturvatehtävissä toimivalta henkilöltä, miten käsite ”tietoturvataso” ymmärretään. Lähes jokainen kuvasi käsitteen eri tavalla. (Valtiovarainministeriö, 2007).

Tietoturvallisuusasetuksessa kuvataan ns. *suojaustasoluokat (ST IV - ST I)* ja kansainvälisiin aineistoihin sovellettavat *turvallisuusluokitukset (TL IV – TL I)*, jotka määrittävät asiakirjojen käsittelyvaatimukset. Nämä vaatimukset kohdistuvat siis asiakirjoihin ja niiden tietojenkäsittely-ympäristöihin. Tietoturvallisuusasetus ei määritä, millaisia toimenpiteitä perustasolla käytännössä tulee toteuttaa. Asetus ei myöskään kerro, millaisia toimenpiteitä perustasoa korkeammat tasot edellyttävät. Asiakirjan siirtämisessä verkossa vaaditaan, että suojaustasoon II (”ST II”) kuuluvan asiakirjan saa siirtää sellaisessa viranomaisen tietoverkossa, jonka käyttö on rajoitettu, jos asiakirja on vahvasti salattu tai se on muutoin vahvasti suojattu ja valtionhallinnon viranomainen on muutoinkin varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät *tavanomaisesti sovellettavan korkean tietoturvallisuustason* vaatimukset.

Valtiovarainministeriö ohjaa valtionhallinnon tietoturvallisuuden kehittämistä valtioneuvoston 26.11.2099 hyväksymällä periaatepäätöksellä. Valtioneuvoston periaatepäätös ohjaa valtionhallinnon organisaatioita soveltamaan Valtionhallinnon tietoturvallisuuden johtoryhmän, eli

VAHTIn ohjeista. Näin ollen tietoturvallisuusasetuksessa mainittu ”tavanomaisesti sovellettava” korkea tietoturvallisuustaso on määritetty VAHTI 2/2010 liitteessä 5. Sellaiset organisaatiot, joita sitovat kansainväliset sopimukset ja tietojenkäsittelyvaatimukset, soveltavat toiminnassaan myös muita tietoturvatasovaatimuksia, kuten KATAKRIa.

Tietoturvallisuusasetus on asettanut tietoturvallisuuden kehittämiselle aikarajoja: ”Viranomaisen tietojenkäsittely on saatettava vastaamaan asetuksen 5§:ssä säädettyjä perustason tietoturvallisuusvaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta.” Tämä tarkoittaa sitä, että perustason tietoturvallisuusvaatimukset tulee täyttyä lokakuussa 2013. Tietoturvallisuusasetus edellyttää korkeamman tietoturvallisuustason saavuttamista viiden vuoden kuluessa, mikäli tämä on päättänyt luokitella asiakirjansa ja käsittelee korkeampaa, kuin ST IV tason tietoaineistoja. Myös toimitilojen on täytettävä vaatimukset tilojen turvallisuudelle viiden vuoden kuluessa asetuksen voimaantulosta. Organisaatiot voivat halutessaan viivytellä perustasoa korkeamman tietoturvallisuustason toimeenpanossa jättämällä tekemättä luokituspäätöksen, mutta se hankaloittaa käytännössä yhteistyötä sellaisten viranomaisten kanssa, joilla luokitusmenettely on käytössä. Viranomaisen tulee tietoturvallisuusasetuksen mukaisesti huolehtia asiakirjaa luovuttaessaan, että vastaanottajalla on riittävät edellytykset (ymmärrys ja turvajärjestelyt) käsitellä asiakirjaa asianmukaisesti.

Tietoturvallisuuden kehittämistyötä tehdään ympäristössä, johon kohdistuu toiminnan tehostamistarpeita. Keväällä 2005 hallitus linjasi, että vain puolet valtionhallinnon poistuman johdosta vapautuvista työpaikoista täytetään. Tämä tarkoittaa sitä, että aikaisempia tehtäviä pyritään suorittamaan entistä pienemmällä henkilömäärällä (VATT 2010). Resursseja kehittämistyöhön on rajallisesti ja käytännönläheistä ”kättä pidempää” on toivottu usean valtionhallinnon organisaation toimesta jo vuodesta 2007 lähtien. Silloin VAHTIn liitteessä 5 esitettyjä tietoturvatasovaatimuksia hahmoteltiin VAHTI:n tietoturvatasot –hankkeessa ensimmäistä kertaa.

Tämän kehittämistehtävän tavoitteena oli laatia menetelmä (vaiheistus, tehtävät ja lopputulokset), jonka avulla organisaatio voi kehittää tietoturvallisuutta sellaisina kokonaisuuksina, joissa sitä on aikaisempaa helpompi hallinta projektin avulla. Menetelmän tueksi laadittiin projektiopas, jossa kerrotaan vaiheittain, miten tietoturvallisuuden kehittämishanketta voidaan viedä eteenpäin. Sekä menetelmä, että projektiopas otettiin vaiheittain käyttöön, ensin kuuden valtionhallinnon organisaation yhteishankkeessa. Tämän jälkeen menetelmää sovellettiin valtiovarainministeriössä ja lopuksi se otettiin oppaineen käyttöön laajemmin Valtiovarainministeriön tietoturvallisuusasetuksen toimeenpanohankkeessa (Asettamispäätös VM 047:15/2007). Sekä projektimalli, että projektiopas ovat vapaasti organisaatioiden käytössä ja projektiopas on veloituksetta ladattavissa mm. www.tietoturvatalkoot.fi –sivustolla.

1.2 Aikaisemmat haasteet tietoturvallisuuden kehittämistyössä

ValtIT:n tietoturvatasot esitutkimushankkeessa selvitettiin vuonna 2007, millaisia tarpeita organisaatioilla on tietoturvallisuuden kehittämisen tueksi. Tuolloin toivottiin käytännönläheistä ”kättä pidempää”, joka neuvoisi, miten käytännön toimenpiteitä toteutetaan. VAHTI laati ohjeen tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010). Ohje ei opasta käytännönläheisesti, miten organisaatio voi edetä tietoturvallisuuden kehittämisessä, vaikka se sisältää paljon hyviä käytänteitä erityisesti tietoaineistojen käsittelyyn. Tietoaineistojen käsittelyosuuden lisäksi ohjeesta sovelletaan laajasti liitettä 5 ”Tietoturvallisuustasojen yksityiskohtaiset vaatimukset.”

Kansallisen auditointikriteeristön soveltamisen tueksi on laadittu ”Kansallisen turvallisuusauditointikriteeristön (KATAKRI) suositusosuuden käyttöohje”. Hyvästä sisällöstä huolimatta, tämäkään ohje ei neuvo askel askeleelta tietoturvallisuuden kehittämistyössä. Organisaatiot joutuvat käytännössä itse suunnittelemaan, miten kokonaisuutta hallitaan. Myös tämän kokonaisuuden soveltamisessa organisaation kehittämistyö voi hankaloitua, koska tehtävien jakaminen ja priorisointi epäonnistuu.

Tässä tutkimuksessa käytännönläheisimmäksi tietoturvallisuuden hallinnan toteuttamisohjeeksi osoittautui ISO/IEC 27003 –standardi (Tietoturvallisuuden hallinnan toteuttamisohjeita). Sen tehtävänä on antaa käytännön opastusta tietoturvallisuuden hallintajärjestelmän (ISMS, *information security management system*) toteuttamissuunnitelman laatimisesta organisaatiossa standardin ISO/IEC 27001:2005 mukaisesti. Ohjeen mukaan ISMS-järjestelmä toteutetaan yleensä projektimuodossa. Ohjeen lähestymistapa valittiin tämän kehittämistehtävän ”punaiseksi langaksi”. Tästä on kerrottu tarkemmin luvussa 1.3.

1.3 Valittu lähestymistapa

Tietoturvallisuuden hallintaan ja siihen liittyviin osiin löytyy useita standardeja. Eräs tunnetuimmista tietoturvallisuuden hallinnan standardeista on ISO/IEC 27001:2005. Soveltaessaan tätä standardia, organisaatio voi halutessaan hakea sen perusteella sertifikaattia. Standardi ei opasta, millä tavoin tietoturvallisuuden hallintajärjestelmä käytännössä toteutetaan. Tämän työn tueksi on laadittu ISO/IEC 27003 –standardi (Tietoturvallisuuden hallinnan toteuttamisohjeita). Sen mukaan tietoturvallisuuden hallinnan toteuttamisen päävaiheet ovat:

A. Johdon hyväksynnän saaminen ISMS-projektin aloittamiselle.
B. ISMS-järjestelmän kattavuuden ja toimintaperiaatteiden määrittely.
C. Organisaation analysointi.
D. Riskien arviointi ja riskien käsittelyn suunnittelu.
E. ISMS-järjestelmän suunnittelu.

Valtionhallinnon organisaatioista harva päätyy kuitenkaan toteuttamaan ISO/IEC 27001 –tasoista tietoturvallisuuden hallintajärjestelmää, vaan monen tarkoituksena on huolehtia siitä, että toiminta saatetaan tietoturvallisuusasetuksen (TTA 681/2010) vaatimalle tasolle. Näin ollen ISO/IEC 27003 –standardi on sellaisenaan sovellettuna liian raskas yleisesti käytettäväksi valtionhallinnossa.

Tässä kehittämistyössä päädyttiin VAHTI 2/2010, KATAKTRIn ja tietoturvallisuusasetuksen (TTA 681/2010) vaatimuksiin peilaten suunnittelemaan mitkä ovat ne päävaiheet, tehtävät ja lopputulokset, jotka organisaation kannattaa toteuttaa lopullisista vaatimuslähteistä riippumatta. ISO/IEC 27003 mukaillen lähestymistapana on projektimallin kuvaaminen. Projektimallin tulee olla yhteensopiva erilaisten vaatimuslähteiden kanssa. Projektimalli kuvataan käytännönläheiseksi oppaaksi ja oppaan tueksi laaditaan työkaluja.

Koska käytännön tilaus projektimallille oli niillä valtionhallinnon organisaatioilla, joilla oli tarkoitus toimeenpanna tietoturvallisuusasetuksen (TTA 681/2010) perustason vaatimukset, projektimallin yhtenä tavoitteena on auttaa organisaatioita saavuttamaan vähintään VAHTI 2/2010 liitteessä 5 kuvattu tietoturvallisuuden perustaso. Vastaavanlainen tavoite olisi voitu asettaa myös KATAKRIn suhteen, mutta se päädyttiin rajaamaan tämän kehittämistehtävän laajuuden vuoksi. Projektimallin tavoitteen määrittäminen edellä kuvatulla tavalla vaikutti siihen, että mallin toimivuutta voidaan myöhemmin arvioida tietoturvatasovaatimusten (VAHTI 2/2010 liite 5) perusteella.

1.4 Tutkimustavoitteet, hyödyt ja rajaukset

Tämän opinnäytetyön tehtävänä oli luoda valtionhallinnon organisaatiossa tietoturvallisuuden kehittämiseen osallistuville kehittämismalli ja opas (metodi) avuksi tietoturvallisuuden hallinnan kehittämiseen. Projektimallin ja oppaan tavoitteina oli jakaa tietoturvallisuuden hallintaan ja kehittämiseen liittyvät tehtävät sellaisiin osiin, että niitä on helppo hallinta ja myöhemmin ylläpitää. Vaikka keittämismallin tehtävänä on ensisijaisesti palvella valtionhallintoa, se on sovellettavissa myös laajemmin esimerkiksi yksityiselle sektorille. Tutkimuksen pääkysymys on: Mitkä ovat tietoturvallisuuden kokonaishallinnan kehittämisen tärkeimmät vaiheet, tehtävät ja lopputulokset?

Kehittämistyö rajattiin koskemaan Suomen valtionhallinnon organisaatioita. Projektimallia sovelletaan alkuvaiheessa niissä organisaatioissa, joilla on tavoitteena toimeenpanna tietoturvallisuusasetuksen (TTA 681/2010) perustason vaatimukset sekä vähintään VAHTI 2/2010 liitteessä 5 kuvatut perustason tietoturvavaatimukset.

Projektimalli ja –opas eivät ole tehty tietyn standardin tai viitekehyksen pohjalta, vaikka niitä on hyödynnetty sisällön suunnittelussa. Tavoitteena oli, että projektimalli ja –opas ovat yhteensopivia erilaisten lähteiden, kuten KATAKRI:n, VAHTI 2/2010 –ohjeen ja tietoturvallisuusasetuksen (681/2010) kanssa. Oppaassa käsitellään vähän projektoinnin perusasioita, sillä lukijan odotetaan joko hallitsevan ne tai hankkivan aiheesta lisätietoja.

1.5 Kehittämisraportin rakenne

Luvussa 2 käsitellään tutkimuksen teoreettista taustaa. Siinä painopisteenä ovat keskeiset kehittämishankkeeseen vaikuttaneet käsitteet ja viitekehykset. Tutkimus- ja kehittämismenetelmät on kuvattu luvussa 3. Painopisteenä on suunnittelutieteisiin kuuluvan konstruktiivisen tutkimus- ja kehittämistavan esittely kehittämishankkeen näkökulmasta.

Luku 4 keskittyy kehittämishankkeen tuloksien esittelyyn ja luvussa 5 tuloksia arvioidaan. Raportin lopussa on yhteenveto. Kehittämistehtävän lopputuloksena syntynyt projektiopas, joka sisältää myös projektimallin, on raportin liitteenä 1.

2 Teoreettinen tausta

Tutkimus jaetaan tavallisesti perus- ja soveltavaan tutkimukseen. Perustutkimuksessa pyritään löytämään vastaus kysymykselle: Millainen maailma on? Soveltavassa tutkimuksessa pyritään ymmärtämään ilmiöiden säännönmukaisuuksia ja piirteitä. (Järvinen & Järvinen 2004) Kehittämistyössä asioiden kuvaaminen ja selittäminen eivät yksinään riitä, vaan niille etsitään parempia vaihtoehtoja.

Kun tarkoituksena on ratkaista käytännön ongelmia ja kehittää uusia ideoita, käytäntöä, tuotteita tai palveluja, puhutaan usein tutkimuksellisesta kehittämistyöstä. Tutkimuksellisessa kehittämistyössä vaaditaan sekä aiheen, että projektihallinnan osaamista. (Ojasalo, Moilanen & Ritalahti 2009). Tässä kehittämistyössä korostuivat erityisesti tietoturvallisuuden, projektihallinnan ja eri viitekehysten osaaminen.

2.1 Keskeiset käsitteet ja määritelmät

2.1.1 Tietoturvallisuus ja tietoturvallisuuden suunnittelu

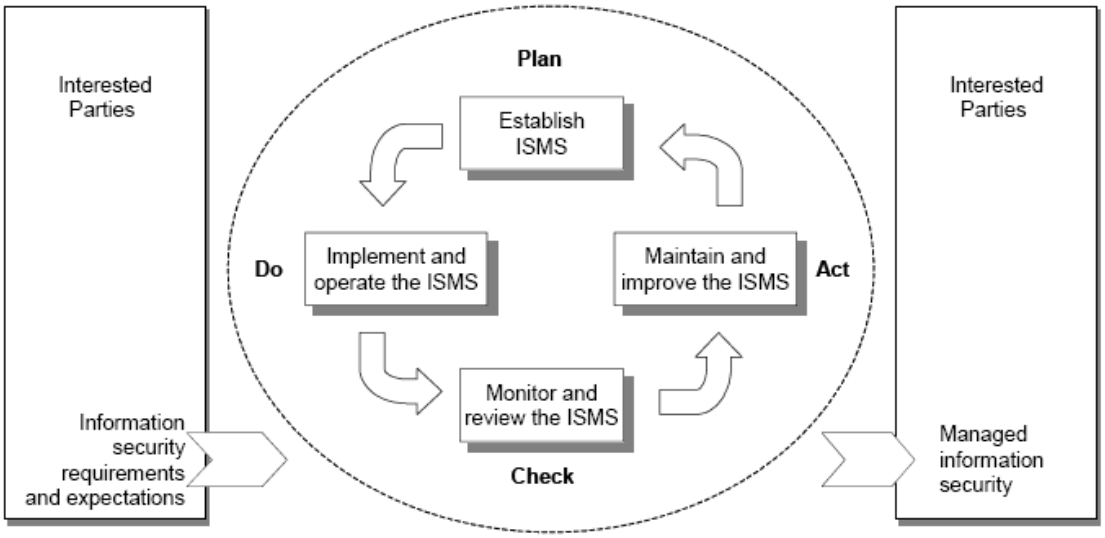
Tietoturvallisuusasetuksessa käsitteellä *tietoturvallisuus* tarkoitetaan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä. (TTA 681/2010)

Asetus tietoturvallisuudesta valtionhallinnossa (681/2010) määrittelee *tietoturvallisuuden suunnittelun* perusteet 2 luvun 4 §:ssä seuraavasti: ”Valtionhallinnon viranomaisen on pidettävä huolta, että tietoturvallisuuden suunnittelu hyvän tiedonhallintatavan mukaisesti perustuu viranomaisen selvityksiin ja arvioihin sen hallussa olevista asiakirjoista sekä niihin talletettujen tietojen merkityksestä ja että suunnittelussa otetaan huomioon vaatimus hyvän julkisuus- ja salassapitorakenteen toteuttamisesta tietojärjestelmissä ja että tietoturvallisuustoimenpiteet mitoitetaan ottamalla huomioon suojattavien tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset.”

2.1.2 Tietoturvallisuuden hallinta ja tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallinta tai *tietoturvallisuuden hallintajärjestelmä* tarkoittaa parhaimmillaan kokonaisvaltaista menettelyä hallita tietoturvallisuutta. Kuviossa 2 on esitetty laajasti sovelletun tietoturvallisuuden hallintajärjestelmästandardin ISO/IEC 27001:2005 näkemys tie-

toturvallisuuden hallintajärjestelmässä. Mallissa olennaisena on hallintajärjestelmän jatkuva kehittäminen.



Kuvio 1 Tietoturvallisuuden hallintajärjestelmä ISO 27001 mukaan. (ISO/IEC 27001, 2005)

VAHTI 3/2007 kuvaa tietoturvallisuuden hallintaa viitekehyksenä, joka koostuu erilaisista toimintamalleista ja dokumenteista, kuten tietoturvallisuutta ohjaavat dokumentit ja suunnitelmat sekä tietoturvallisuuden raportointi ja arviointimenettelyt. Hallintajärjestelmän tehtävänä on toteuttaa organisaation strategiaa. Sen avulla seurataan ja arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta.

Kuvio 2 Tietoturvallisuuden hallintajärjestelmän malli VAHTI 3/2007 mukaan.
VAHTI 3/2007 mukaan tietoturvallisuuden hallintajärjestelmän olennaisimmat osat ovat ajantasainen tietoturvapolitiikka ja siihen liittyvät asiakirjat sekä säännöllinen riskienhallinta, joka koskee sekä nykyistä toimintaa että suunniteltuja muutoksia. (VAHTI 3/2007)

2.1.3 Tietoturvatasot ja suojattavat kohteet

Tietoturvatason avulla voidaan määrittää vähimmäisvaatimukset suojattavien kohteiden turvaamiseksi. Tietoturvatasolla voidaan myös tarkoittaa laajempaa tietoturvallisuuden hallinnan kokonaisuutta.

Tietoturvallisuusasetuksessa määritetään *tietoturvallisuuden perustaso*. Se on kymmenen kohdan vaatimusluettelo erilaisista tietoturvallisuuteen liittyvistä toimenpiteistä (ks. luku 1.1). Asetuksessa kuvataan kuitenkin muitakin tietoturvallisuusluokituksia. Esimerkiksi 3 luvussa käsitellään asiakirjojen luokittelua. Luokitusten perusteet on kuvattu 8§:ssä seuraavasti: ”Salassa pidettävät asiakirjat tai niihin sisältyvät tiedot voidaan luokitella sen mukaan, mitä tietoturvallisuutta koskevia vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Luokittelu voidaan suorittaa myös siten, että tietoturvallisuutta koskevat vaatimukset kohdistetaan vain sellaisiin asiakirjoihin tai sellaisiin asiakirjan käsittelyvaiheisiin, joissa erityistoimenpiteet ovat suojattavan edun vuoksi tarpeen. Luokitusta ei saa ulottaa sellaiseen asiakirjaan tai asiakirjan osiin, joissa käsittelyvaatimusten noudattaminen ei suojattavan edun vuoksi ole tarpeen. Muu kuin salassa pidettävä asiakirja voidaan luokitella vain 9 §:n 2 momentissa tarkoitetuissa tapauksissa.”

ISO/IEC 27002 –standardin mukaan suojattavat kohteet käsittävät palvelut, mutta ei toimintoja ja prosesseja yleisesti. Suojattavien kohteiden tyypit voidaan jakaa ISO/IEC27002 –standardin mukaan seuraavasti:

- henkilöt
- tilat
- laitteet
- tietoliikenne ja tietojärjestelmät (sis. rekisterit ja tietokannata)
- palvelut
- tietoaineistot (kaikissa muodoissa).

KATAKRI (Kansallinen auditointikriteeristö) käsittelee tietoturvaluokituksia kriteereinä luottamuksellisuuden, eheyden ja käytettävyyden näkökulmasta. Tietoturvakriteeristö on jaettu neljään tasoon. Tasot ovat lähtötason suositukset, perustason vaatimukset (IV), korotetun tason vaatimukset (III) ja korkean tason vaatimukset (II). Alin taso, lähtötason suositukset,

koskee koko organisaation kohteiden turvaamista sekä tietoturvallisuuden kokonaishallintaa. Tasojen IV-II vaatimukset koskevat vain suojattavaa kohdetta. Suojattavalla kohteella tarkoitetaan suojattavaa tietoa sekä sen käsittely-ympäristöä.

2.2 Tutkimuksessa sovelletut tärkeimmät viitekehykset

2.2.1 ISO/IEC 27000 –standardisarja

ISO/IEC 27000 –standardisarja käsittelee monipuolisesti tietoturvallisuuden hallintaa. Sarjasta vastaa kansainvälinen ISO/IEC JTC 1/SC 27 -komitea. Suomen osalta komitean ja sen työryhmien työ seuraa SFS:n tietoturvastandardien seurantaryhmä 307. Ryhmä osallistuu kansainväliseen standardointityöhön mm. tekemällä kannanottoja. Tämän kehittämistyön laatimishetkellä ISO/IEC – standardisarja jakautui yhdeksään osa-alueeseen. Näistä yksi laajimmin käytetyistä standardeista on ISO/IEC 27001 –standardi. Kyseistä standardia soveltava organisaatio voi hakea tietoturvallisuuden hallintajärjestelmälleen ISO 27001 –sertifikaattia. Tässä kehittämistyössä sovellettiin erityisesti ISO/IEC 27001 –käyttöönottoa ohjeistavaa ISO/IEC 27003 –standardia.

2.2.2 Asetus tietoturvallisuudesta valtionhallinnossa

Asetus tietoturvallisuudesta valtionhallinnossa (681/2010) julkistettiin 1.7.2010 ja se astui voimaan 1.10.2010. Asetusta kutsutaan yleisesti nimellä ”tietoturvallisuusasetus”. Asetus selkeytti valtionhallinnon organisaatioiden tietoturvallisuuden kehittämistavoitteita: Jokaisen organisaation tulee toteuttaa tietoturvallisuuden perustaso 1.10.2013 mennessä. Perustason vaatimukset on kuvattu tämän raportin johdannossa.

Tietoturvallisuusasetus määrittää tietoturvatasojen lisäksi luokitukset myös tietoaineistojen salassapidolle. Luokituksia on käytännössä kaksi:

1. suojaustasoluokitus, jossa suojaustasot ovat
    a. suojaustaso IV (ST IV)
    b. suojaustaso III (ST III)
    c. suojaustaso II (ST II)
    d. suojaustaso I (STI)
2. turvallisuusluokitus, jossa turvallisuusluokat ovat
    a. turvallisuusluokka IV (TL IV), Käyttö rajoitettu
    b. turvallisuusluokka III (TL III), Luottamuksellinen
    c. turvallisuusluokka II (TL II), Salainen
    d. turvallisuusluokka I (TL I), Erittäin salainen.

Tietoturvallisuusasetuksessa edellytetään, että tietoaineistojen käsittely-ympäristön tulee vastata tietoaineiston vaatimaa suojaustasoa. Käytännössä tämä tarkoittaa sitä, että suojaustason IV tietoaineistoja voi käsitellä perustason täyttävässä tietojenkäsittely-ympäristössä. Vastaavasti suojaustasoa IV korkeampaa turvaluokkaa käsittelevien organisaatioiden tulee toteuttaa perustason lisäksi kyseistä suojaustasoa vastaavat korkeammat turvamenettelyt. Tietoturva-asetuksessa ei kuitenkaan ole määritetty, mitä lähdettä perustasoa korkeammassa turvatasossa tulee soveltaa, vaan siinä käytetään määritelmää ”tavanomaisesti sovellettavan korotetun tietoturvallisuustason vaatimukset”.

2.2.3 VAHTI 2/2010

Valtiovarainministeriön Ohjeen tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta tavoitteena on tehostaa ja yhdenmukaistaa lain viranomaisen toiminnan julkisuudesta (621/1999) perusteella tietoturvallisuusasetuksen täytäntöönpanoa. Ohjeen mukaisella toiminnalla viranomainen voi saavuttaa toiminnassaan ja yhteistyössään asetuksen mukaisen tietoturvatason, joka tasapainottaa riskienhallinnan ja kustannustehokkuuden. VAHTI 2/2010 –ohjeen liitteessä 5 on kuvattu tietoturvatasovaatimukset perustasolle, korotetulle tasolle ja korkealle tasolle. (Lähde www.vm.fi)

2.2.4 KATAKRI

KATAKRI, eli kansallinen turvallisuusauditointikriteeristö on laadittu yhtenäistämään viranomaistoimintoja silloin, kun viranomainen toteuttaa organisaatiossa turvallisuustason todentavan tarkastuksen, auditoinnin. Kriteeristön toisena tavoitteena on auttaa organisaatioita turvallisuuden kehittämistyössä. Vuonna 2009 julkaistussa versiossa keskityttiin ns. security-turvallisuuteen. KATAKRIa päivitettiin opinnäytetyön laatimisen aikana. Opinnäytetyössä käytettiin lähteenä 20.11.2009 versiota.

Turvalisuusauditointikriteeristö jakautuu neljään osa-alueeseen: hallinnollinen turvallisuus (turvallisuuskohtaminen), henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Jokaiselle osa-alueelle on laadittu kolmiportainen vaatimusluokittelu, joka vastaa turvallisuustasokäsitteitä perustaso, korotettu taso ja korkea taso. Kriteeristö on laadittu ehdottomien vaatimusten näkökulmasta. (Lähde: http://www.defmin.fi/files/1525/Katakri.pdf)

2.3 Yhteenveto tärkeimmistä viitekehyksistä

Tietoturvallisuuden tason parantamiseen liittyy useita eri viitekehyksiä. Edellä kuvatut viitekehykset eivät kuitenkaan ole suoraan toisiinsa rinnastettavissa, vaikka organisaatiot soveltaisivat niistä useampaa omassa toiminnassaan.

Tietoturvallisuusasetusta (TTA 681/2010) lukuun ottamatta muita luvussa 2 esitettyjä viitekehyksiä oltiin kehittämässä tätä kehittämistyötä tehtäessä. KATAKRIsta julkaistiin uusi versio keväällä 2011, kesäkuussa käsiteltiin Suomen standardointiliiton toimesta ISO/IEC 27001 – standardin päivitysehdotusta ja VAHTI 2/2010 liitteen 5 tietoturvavaatimusten kehittämisestä tehtiin esitys Valtion IT-palvelukeskuksen toimesta syksyllä 2011. Koska viitekehykset ja vaatimuslähteet muuttuvat, kannattaa myös tietoturvallisuuden hallintajärjestelmä mahdollistaa uusien vaatimusten huomioimisen mahdollisimman joustavasti.

3 Tutkimus- ja kehittämismenetelmät

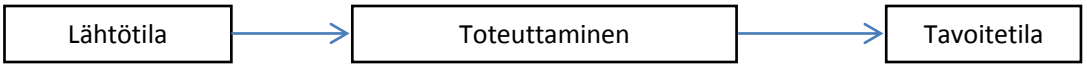
Kehittämistyössä tutkimuksellisuus on tärkeää muun muassa siksi, että sen avulla kehittämistyöhön vaikuttavat tekijät otetaan tavallista kattavammin ja suunnitelmallisemmin huomioon ja kehittämistyön tulokset ovat paremmin perusteltavissa.(Ojasalo, Moilanen & Ritalahti 2009)

Pertti ja Annikki Järvinen käsittelevät kirjassaan ”Tutkimustyön metodeista” suunnittelutieteisiin kuuluvaa konstruktiivista tutkimusta laajasti. Kirjan luvussa 5 pyritään vastaamaan kysymyksiin: ”Voimmeko rakentaa tietyn innovaation ja kuinka hyödyllinen on joku innovaatio?”. Vaikka tässä kehittämistyössä ei tavoitteena ollut saada aikaiseksi innovaatiota, Järvisten lähestymistapa sopi tutkimuksen toteutukseen hyvin. (Järvinen & Järvinen, 2004)

3.1 Menetelmällinen perusta

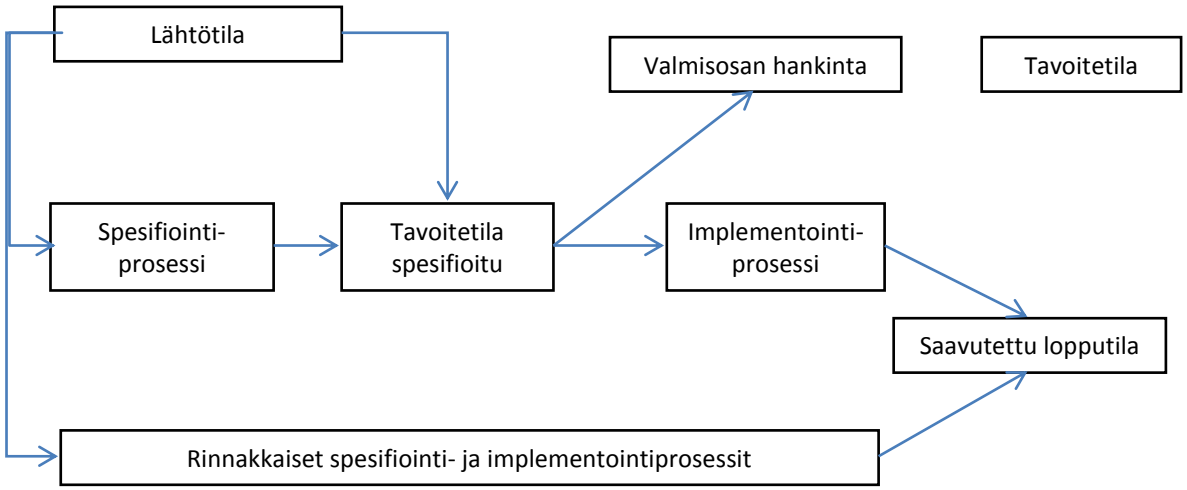
Konstruktiivinen tutkimus, eli suunnittelutieteellinen tutkimus sopii kehittämistehtävään, jolla on konkreettinen tuotos, kuten suunnitelma, mittari tai malli. Tutkimuksessa pyritään hyvin käytännönläheiseen ongelmanratkaisuun luomalla uusi rakenne tai luomalla jotakin uutta aikaisemman tutkimustiedon pohjalta. (Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009, s. 65)

Järviset esittävät, että innovaation toteuttaminen käsittää metodin, jonka avulla saadaan aikaiseksi muutoksen lähtötilasta tavoitetilaan. Järvisten mukaan tavoitetilan kuvaus on malli siitä tilanteesta, jossa toivomme asioiden olevan, kun olemme realisoineet ideamme (kuvio 3).



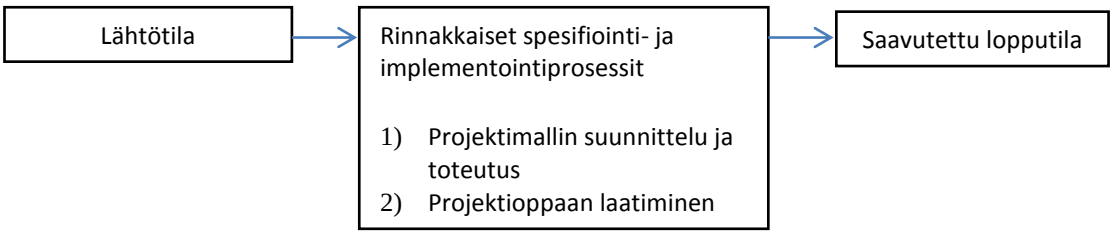
Kuvio 3. Innovaation toteuttamisprosessi (Järvinen & Järvinen, 2004, 107)

Lähtötilasta voidaan Järvisten mukaan pyrkiä tavoitetilaan ainakin kolmea polkua pitkin (kuvio 4). Kuviossa mielenkiintoinen osa on ”Valmisosan hankinta”. Järvisten mukaan valmisosa kannattaa joskus hankkia, jolloin pyörää ei tarvitse keksiä uudelleen.



Kuvio 4. Vaihtoehtoisia tapoja toteuttaa innovaatio (Järvinen & Järvinen 2004, 108)

Tässä kehittämistyössä päädyttiin toteuttamisvaiheessa rinnakkaiseen spesifointi- ja implementointiprosessiin (kuvio 5).



Kuvio 5. Kehittämistyön vaiheet karkealla tasolla

Projektimallin suunnittelu ja toteutus tapahtui seuraavissa vaiheissa:

1. Lähtötietojen kerääminen, esitutkimus.
2. Karkean tason hahmotelma projektimallin osista.
3. Metodin vaiheiden esittely pienryhmälle sekä asiantuntijaverkostolle, palautteen ja kehitysehdotusten kokoaminen.
4. Karkean tason hahmotelman muokkaaminen palautteen perusteella.
5. Valmiin projektimallin osien esittely ja käyttöönotto.

Projektioppaan laatiminen tapahtui seuraavissa vaiheissa:

1. Lähtötietojen kerääminen, esitutkimus.
2. Projektioppaan sisällön luonnoksen hahmottelu projektimallin avulla.
3. Sisältöluonnoksen vertaaminen valittuihin viitekehyksiin.
4. Projektioppaan luonnoksen tuottaminen.
5. Luonnoksen esittely pienryhmälle sekä asiantuntijaverkostolle.
6. Luonnoksen muokkaaminen kommenttien perusteella.

7. Uuden luonnoksen esittely laajemmalle asiantuntijaryhmälle.
8. Luonnoksen muokkaaminen kommenttien perusteella.
9. Sisältöluonnoksen vertaaminen uudelleen valittuihin viitekehyksiin.
10. Lopullisen projektioppaan käyttöönotto.

Edellä kuvattu malli on esitetty karkealla tasolla. Käytännössä usea organisaatio otti projektioppaan käyttöön jo luonnosvaiheessa, jolloin niille toimitettiin myöhemmin päivitetty versio. Tämän mahdollisti projektimallin (vaiheet, tehtävät ja lopputulokset) huolellinen suunnittelu, jolloin projektioppaan sisältö kasvoi, mutta rakenne pysyi käytännössä samanlaisena. Keskeneräisen projektioppaan käyttöönotto kertoo osaltaan siitä, että se oli tarpeellinen.

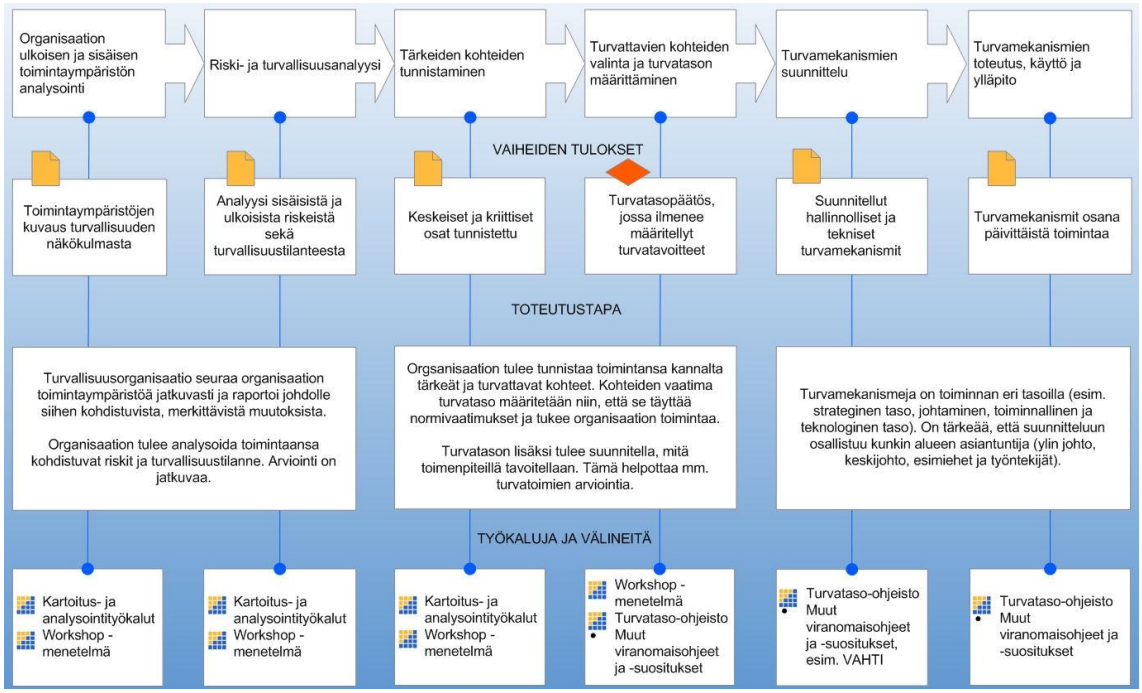
Projektimallia ja projektiopasta sovellettiin käytännön tasolla (implementoitiin) valtiovarainministeriön sisäisessä tietoturvallisuuden kehittämishankkeessa, jossa menettelytapojen lisäksi lopputuloksena saatiin aikaiseksi koko tietoturvallisuuden hallinnan kuvaava tietoturvakäsikirja. Viimeisessä vaiheessa projektimalli ja – opas otettiin käyttöön valtiovarainministeriön asettamassa tietoturvallisuusasetuksen toimeenpanon yhteishankkeessa.

3.2 Lähtötila

Valtiovarainministeriössä käynnistettiin ValtIT:n toimesta tietoturvatasojen esitutkimushanke vuoden 2006 lopussa. Esitutkimus suoritettiin virkamiesten työryhmätyöskentelynä, jossa käytettiin ulkoisia asiantuntijoita. Oma roolini oli toimia ulkoisena, päävastuullisena asiantuntijana maaliskuusta 2007. Tehtäväni oli tukea ryhmää työskentelyssä sekä hankkia tietoa lopullista hankeraporttia varten.

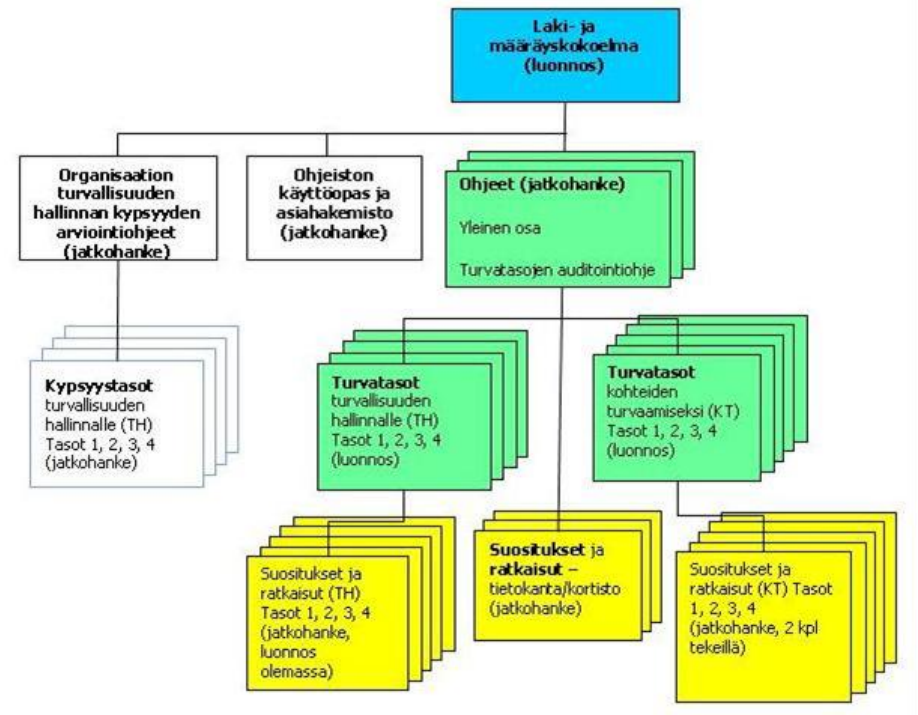
Tietoturvatasot-esitutkimuksessa havaitiin, että hallinnossa jokaisella työntekijällä on yksilöllinen näkemys, siitä mitä tietoturvallisuus omassa työssä tarkoittaa. Myös tietoturvallisuuden hallintaa tukevat toimet eri hallinnonaloilla ja virastoissa poikkesivat osittain. Hankeryhmä selvitti valtionhallinnon turvallisuuden vähimmäisvaatimuksia ja arvioi muita kansallisia sekä kansainvälisiä kriteeristöjä sekä standardeja. Hankeryhmä keräsi myös toiveita siitä, millaisia olisivat VM:n hallinnolle tarjoamat tietoturvallisuuteen liittyvät yhteiset rakenteet, palvelut ja välineet. (www.vm.fi)

Esitutkimuksen yhteydessä tutustuin suureen määrään tietoturvallisuuden hallintaa koskeviin kirjoituksiin, standardeihin ja viitekehyksiin. Tuolloin syntyivät ensimmäiset ajatukset valtionhallinnolle suunnatusta tietoturvallisuuden hallintaoppaasta. Esitin työryhmälle hankkeen aikana alustavan version tietoturvallisuuden hallinnan ohjeistuksen rakenteesta ja tietoturvallisuuden hallinnan projektoinnin vaiheistuksesta.



Kuvio 6. Tietoturvatasot -esitutkimushankkeessa laadittu luonnos tietoturvallisuuden kehittämisen vaiheistuksesta.

Tietotuturvatasot –esitutkimushankkeessa hahmoteltiin ohjeistorakenne tukemaan tietoturvallisuuden kehittämistyössä (kuvio 7).



Kuvio 7. Tietoturvatasot -esitutkimushankkeessa hahmoteltu ohjeistoluonnos. (Valtiovarainministeriö 2007, 40)

Vuonna 2009 toimin tietoturvaosuuden asiantuntijana Kansallisen tietoturva-auditointikriteeristön (KATAKRI) laatimisessa. Tuolloin havaitsin, että useat valtionhallinnon organisaatiot joutuvat soveltamaan eri kriteeristöjä toiminnassaan. Tuolloin asetus tietoturvallisuudesta valtionhallinnossa (TTA 681/2010) oli vielä luonnosvaiheessa, mutta tasorakenne oli jo muodostunut. Samaan aikaan seurasin tietoturvastandardien kehittymistä SFS:n tietoturvastandardien seurantaryhmässä.

Elokuussa 2010 aloitin työskentelyn Valtion IT-palvelukeskuksessa. Sain tehtäväkseni toimia asiantuntijana kuuden valtinhallinnon organisaation yhteishankkeessa. Tämän hankkeen ryhmä toimi alkuvaiheessa projektimallin arvioijana. Organisaatioiden tavoitteena saavuttaa VAHTI 2/2010 tietoturvatasovaatimusten hallinnollisen kriteeristön korotettu taso. Tässä hankkeessa tuettiin organisaatioita tason saavuttamisessa. Tällöin syntyi ensimmäinen konkreettinen tarve projektimallille- ja oppaalle. Toinen kehittämistehtävä alkuun paneva voima oli tietoturva-asetuksen (TTA 681/2010) voimaan astuminen lokakuussa 2010. Vuoden 2010 lopussa aloitin osa-aikaisena tietoturvapäällikkönä valtiovarainministeriössä. Näin pääsin organisaatioon, jossa käytännössä pääsisin itse soveltamaan projektimallia ja – opasta.

3.3 Tavoitetila

Tietoturvatasot –esitutkimuksen yhteydessä syntyivät ensimmäiset ajatukset valtionhallinnolle suunnatusta tietoturvallisuuden hallintaoppaasta. Samaan aikaan esitin alustavan version tietoturvallisuuden hallinnan ohjeistuksen rakenteesta ja tietoturvallisuuden hallinnan projektoinnin vaiheistuksesta.

Tämän kehittämistehtävän tavoitteeksi muodostuivat kaksi tehtävää:

1. Tietoturvallisuuden hallinnan toteutusmenetelmän (metodi, malli) laatiminen (vaiheistus, tehtävät ja lopputulokset).
2. Menetelmän tueksi laadittavan projektioppaan laatiminen.

Tietoturvallisuuden hallinnan toteutusmenetelmän avulla organisaatio voi kehittää tietoturvallisuutta sellaisina kokonaisuuksina, joissa sitä on aikaisempaa helpompi hallinta projektin avulla. Mallissa tähdätään siihen, että se palvelee mahdollisimman monenlaisia valtionhallinnon organisaatioita ja se on yhteensopiva erilaisten vaatimuslähteiden kanssa.

Projektioppaan tehtävänä oli opastaa käytännönläheisesti toteuttamaan tietoturvallisuuden hallintajärjestelmä vaihe vaiheelta. Oppaan tulisi olla yhteensopiva ainakin tietoturvallisuusasetuksen (TTA 681/2010), VAHTI 2/2010 liitteen 5 tietoturvatasovaatimusten sekä KATAKRIn (Kansallinen auditointikriteeristö) kanssa. Yhteensopivuudella varmistettaisiin, että se tukee

eri vaatimusten toteuttamista, mutta ei kuitenkaan tee tietoturvallisuuden hallintakokonaisuudesta liian jäykkää.

Lopullisesti tavoitetilaksi muodostuivat seuraavat asiat:

- Kehittämishankkeessa luodaan projektimalli (metodi). Mallin tulee olla selkeä ja sen tulee jakaa kokonaisuuden sellaisiin kokonaisuuksiin, jossa se on mahdollisimman helppo toteuttaa sekä myöhemmin ylläpitää;
- Projektimalli on hyödynnettävissä erilaisissa organisaatioissa;
- Projektioppaan rakenne ja ulkoasu on selkeä;
- Projektioppaan sisältö on selkeä.

3.4 Toteuttaminen

Tutkimus- ja kehityshanke toteutettiin rinnakkaisina spesifiointi- ja implementointiprosesseina. Vaikka projektimallin suunnittelu ja projektioppaan laatiminen voidaan karkeasti jakaa kahdeksi kokonaisuudeksi, tapahtui niiden käyttöönotto käytännössä vaiheittain.

3.4.1 Projektimallin suunnittelu ja toteutus

Projektimallin tehtävänä oli jakaa tietoturvallisuuden kehittämistyö sellaisiksi kokonaisuuksiksi, tehtäviksi ja lopputuloksiksi, joissa ne on aikaisempaa helpompi toteuttaa ja hallita. Työ aloitettiin keräämällä lähtötietoja ja etsimällä sellaisia viitekehyksiä, joista olisi hyötyä.

Parhaimmaksi sovellettavaksi viitekehykseksi projektimallin suunnittelussa osoittautui ISO/IEC 27003 –standardi. Standardin tarkoitus on opastaa tietoturvallisuuden hallintajärjestelmän (engl. ISMS, Information Security Management System) toteuttamisessa standardin ISO/IEC 27001:2005 mukaisesti. Standardi ei käsittele operatiivisia toimintoja, vaan suunnittelua, jonka lopputuloksena on tietoturvallisuuden hallintajärjestelmän toteuttamissuunnitelma. Projektimallin tehtävänä oli nimenomaan auttaa tietoturvallisuuden hallinnan toteuttamisessa. Koska ISO/IEC 27003 – standardi on tarkoitettu palvelemaan ISO/IEC 27001 – standardin toteuttamista, se oli paikoin liian raskas sovellettavaksi laajamittaisesti valtionhallinnossa. Sen vuoksi standardista päädyttiin poimimaan parhaiten toimivat ideat. Standardi vaiheistaa tietoturvallisuuden hallinnan toteuttamisen seuraaviin päävaiheisiin:

A. Johdon hyväksynnän saaminen ISMS-projektin aloittamiselle.
B. ISMS-järjestelmän kattavuuden ja toimintaperiaatteiden määrittely.
C. Organisaation analysointi.
D. Riskien arviointi ja riskien käsittelyn suunnittelu.
E. ISMS-järjestelmän suunnittelu.

Tein standardin pohjalta alustavan hahmotelman neljästä eri osa-alueesta. Nimesin osa-alueet kirjaintunnuksin A-D (kuvio 8). Näin kunkin osa-alueen sisälle jääville osille voitiin antaa tarkemman tason tunnukset (A1-An). Varmistin, että projektimallissa huomioidaan VAHTI 2/2010 liitteen 5 tietoturvatasovaatimukset (taulukko 5).

VAHTI 2/2010 liitteen 5 tietoturvatasovaatimus	Liittyy projektimallin tehtävään
1.1.1.1. Perustaso Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.	A1, A3, D5, D6
1.1.1.2. Perustaso Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.	A3, B2
1.1.1.3. Perustaso Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.	B5, D5, D7
1.1.1.4. Korotettu taso Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.	A3, A4, D5, D8, F

Taulukko 1 VAHTI 2/2010 vertaaminen projektimallin tehtäviin.

KATAKRIssa on VAHTI 2/2010 liitteen 5 tavoin eri vaatimustasoja. Koska eri kriteeristöt eivät ole suoraan keskenään verrattavissa, ei ollut tarkoituksenmukaista tutkia KATAKRIn eri kysymysten sisäisiä vaatimustasoja. Sen vuoksi kriteeristön vaatimuksista laadittiin lista kunkin vaatimuksen pääasiallisen sisällön mukaan. Taulukossa 5 näkyy, miten vaatimukset A 101 ja A 102 on yksinkertaistettu. Samoin taulukossa on esitetty, miten vaatimukset liittyvät projektimallin eri tehtäviin.

	KATAKRI	Liittyy projektimallin tehtävään
A 101	Johdon tukema ja tarkistama turvallisuuspolitiikka	B5, D7
A 102	Turvallisuuspolitiikan ja/tai turvallisuuden johtamisen riittävän kattavuuden varmistaminen turvallisuusdokumentaatiossa	A2, B1, B3, B4, C5, D2

Taulukko 2 KATAKRIn vuoden 2009 kriteerit A 101.9 ja A 102.0 yksinkertaistettuna sekä yhdistettyinä projektimallin osiin

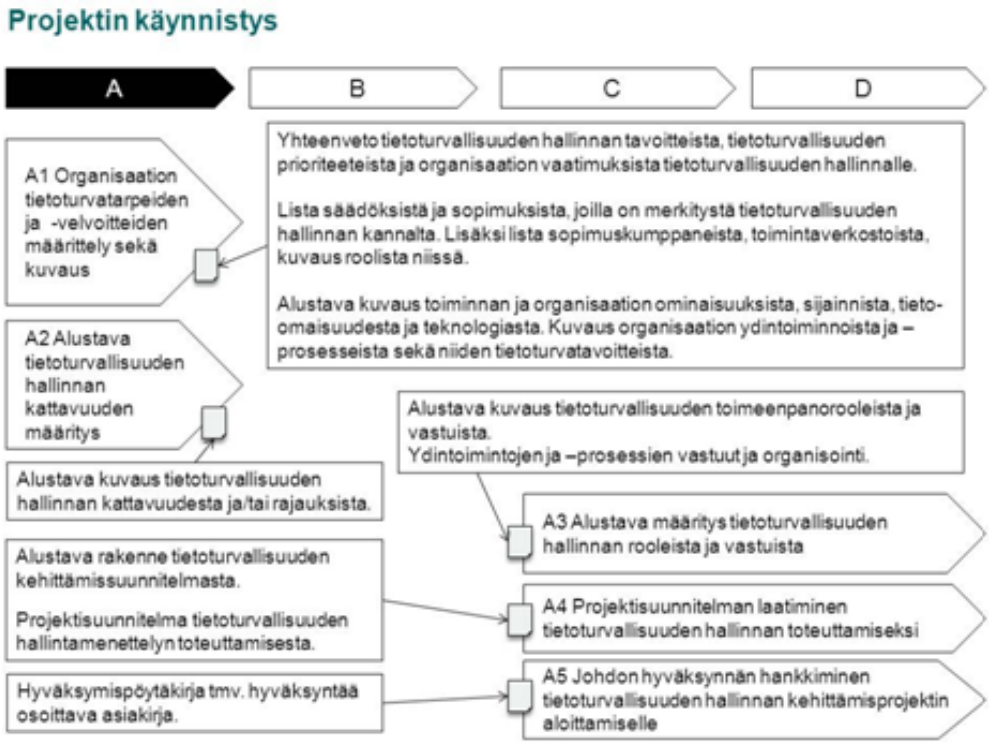
Kun projektimallin rakenne ja työvaiheet tehtävineen oli määritelty ja kuvattu alustavasti, tarkastettiin kunkin vaiheen yhteensopivuus ISO/IEC 27001:n, Tietoturvallisuusasetuksen (681/2010), VAHTI 2/2010 ja KATAKRIin nähden (ks. taulukko 5). Vaikka ISO/IEC 27001 – standardia ei alun perin valittu suoraan projektimallissa sovellettavaksi viitekehykseksi, haluttiin varmistaa, että malli on yhteensopiva ko. standardin kanssa.

Vaihe	Lopputulos	ISO 27001	TTA luku 2	VAHTI 2/2010	KATAKRI
A Tietoturvatarpeiden ja lähtökohtien tunnistaminen					
A1 Organisaation tietoturvatarpeiden, -velvoitteiden ja tavoitteiden määrittäminen sekä kuvaaminen	Luettelo/kuvaus tietoturvallisuuden kannalta merkittävistä ▫ sopimuksista, ▫ velvoitteista, ▫ organisaation ydintavoitteista, ▫ organisaation johtamisjärjestelmistä ja ▫ kuvaus organisaation tärkeimmistä tietoturvatavoitteista	4.2.1a) A15.1.1	4§	1.1.1., 2.2.3., 2.5.1., 3.1.1.	A105, A108, A301, A302, A305, A505, I108
A2 Alustava tietoturvallisuuden hallinnan kattavuuden määritys	Alustava kuvaus tietoturvallisuuden hallinnan kattavuudesta		4§		A102
A3 Alustava määritys tietoturvallisuuden hallinnan rooleista ja vastuista	Alustava kuvaus tärkeimmistä toiminnoista, rooleista ja vastuista.	4.2.2g), A.6.1.3, A.7.1.1, A.7.1.2, A.8.1.1, A.8.1.3, A.9.2.6, A.10.1.1, A.10.7.2, A.12.5.1,	5§2) 5§3)	1.1.2. 1.2.1. 1.4.1., B4, C2	A504, A505
A4 Projektisuunnitelman laatiminen tietoturvallisuuden hallinnan toteuttamiseksi	Projektisuunnitelma	ISO 27003			
A5 Johdon hyväksynnän hankkiminen projektin aloittamiselle	Hyväksymispöytäkirja tmv.	5.1a)-h)			A505, I101

Taulukko 3 Hahmotelma projektimallin tehtävistä ja niiden vastaavuus eri lähteisiin nähden.

Esittelin alustavan hahmotelman projektimallin osista pienryhmälle syyskuussa 2010. Kirjoitin ylös pienryhmän jäsenten kommentit ja kehittämisehdotukset. Pienryhmä koostui kuuden organisaation tietoturvallisuudesta vastaavasta henkilöstä. Organisaatiot osallistuivat tietoturvallisuuden kehittämishankkeeseen. Hankkeen tavoitteena oli kehittää hankkeeseen osallistuvien organisaatioiden tietoturvallisuutta ja parantaa valmiuksia saavuttaa VAHTI 2/2010 liitteessä 5 kuvattu korotettu tietoturvataso 30.9.2013 mennessä.

Lähetin sähköpostitse alustavan hahmotelman muutamille tietoturvallisuuden hallinnan asiantuntijoille kommentoitavaksi. Huomioin myös tästä kommenttikierroksesta saadut palautteet projektimallin suunnittelussa.



Kuvio 8. Ensimmäinen esitelty hahmotelma osa-alueesta A

Saamieni palautteiden perusteella hahmottelin lopullisen version (ks. liiteen 1 taulukko 4). Tämän version tehtävänä oli muodostaa vaiheet tietoturvallisuuden hallinnan kehittämisprojektille. Projektimalli hyväksyttiin käytettäväksi pienryhmän yhteishankkeessa. Tässä yhteydessä yhteishankkeen hankesuunnitelma vaiheistus päivitettiin vastaamaan projektimallin vaiheistusta. Valitsin projektimallin avuksi muodostamaan rungon projektioppaalle. Laadin myös valtiovarainministeriön tietoturvallisuuden kehittämishankkeen projektimallin vaiheiden mukaisesti.

3.4.2 Projektioppaan laatiminen

Projektiopasta varten tutkin runsaasti tietoturvallisuuden hallinnan peruskirjallisuutta. Hyödynsin paljon myös vuosien varrella keräämääni omaa aineistoa ja käytännön työkokemusta. Projektioppaan sisällön rungon hahmottelin projektimallin mukaisesti (taulukko 2). Tutkin muita oppaita ja luonnostelin niiden perusteella oppaan muun rakenteen.

Projektioppaan sisältöä kirjoitin vuoroin oman työkokemuksen ja osaamisen perusteella, keskustellen muiden asiantuntijoiden kanssa sekä poimimalla tärkeitä kohtia valituista viitekehyksistä (VAHTI 2/2010 liite 5, KATAKRI ja TTA 681/2010). Pyrkimyksenä oli pitää kirjoitettu teksti mahdollisimman ytimekkäänä ja käytännönläheisenä. Kun projektioppaan ensimmäinen luonnos oli valmis, varmistin että valitut viitekehykset tulee riittävästi huomioitua tekstissä. Käytin taulukossa 5 esitettyä tapaa tarkistaa projektioppaan ja lähteiden vastaavuus. Tein

myös tarkastelun taulukoissa 2 ja 3 esitetyllä tavalla. Tämän jälkeen lähetin luonnoksen kommentoitavaksi pienelle tietoturvallisuuden hallinnan asiantuntijaverkostolle.

Esittelin projektimallin ja opasluonnoksen Valtion IT-palvelukeskuksen asiakaspäivillä 31.3. Pyysin halukkaita ilmoittautumaan arvioimaan ja kommentoimaan opasta. Kymmenen henkilöä ilmoittautui. Tämän lisäksi lähetin oppaan myös muutamalle muulle asiantuntijalle ja tietoturvallisuudesta vastaavalle. Opasta täydennettiin vielä hieman.

Lähetin lähes valmiin oppaan kommentoitavaksi kymmeneen organisaatioon. Sain palautteet oppaan arviointia varten viidestä organisaatiosta (ks. luku 4). Arviot olivat laadullisia, vaikka arviointiin käytettiin kouluarvosanoja. Sen vuoksi arvio on suuntaa antava.

Arvosana viidestä valtionhallinnon organisaatiosta (1-5) kouluarvosanoin	Arvosana					Keskiarvo
Projektimallin selkeys ja tapa jäsentää kokonaisuus	5	3	4	5	4	4,2
Projektimallin hyödynnettävyys omassa organisaatiossa	5	3	3	5	4	4
Projektioppaan selkeys, rakenne ja ulkoasu	5	3	3	4	4	3,8
Projektioppaan sisältö	5	4	4	5	4	4,4
Projektioppaan hyödynnettävyys omassa organisaatiossa	5	3	4	5	4	4,2
Yhteensä						4,12

Taulukko 4 Projektimallin ja oppaan arviointi.

Paransin opasta saamani palautteen perusteella. Tämän jälkeen lähetin oppaan kommentoitavaksi laajemmalle asiantuntijaryhmälle huhtikuussa 2011. Muokkasin jälleen opasta kommenttien perusteella. Tämän jälkeen tarkistin vielä kerran sisällön valittuihin viitekehyksiin nähden. Projektimallia ja –opasta soveltaneille organisaatioille lähetettiin päivitetty opas uudemman version valmistuttua.

3.5 Saavutettu lopputila

Kehittämishankkeessa luotiin projektimalli (metodi), joka otettiin käyttöön erilaisissa valtionhallinnon organisaatioissa. Tämän lisäksi laadittiin projektiopas, joka oli palautteen mukaan riittävän selkeä hyödynnettäväksi niin organisaation itsenäisessä kehittämistyössä, kuin yhteishankkeissa. Tätä raporttia laadittaessa organisaatioiden tietoturvallisuuden kehittämistyö oli vielä kesken, joten kattavaa kuvaa lopputilasta ei voida muodostaa. Työn arviointia on tarkemmin käsitelty luvussa 5.

4 Kehittämistulokset

Tässä kehittämishankkeessa lähdettiin siitä olettamuksesta, että valtionhallinnossa ei ole organisaatioiden vapaaseen käyttöön selkeää etenemismallia (projektimallia), jonka avulla organisaatio voi kehittää tietoturvallisuuden hallintaa. Aiheesta ei myöskään löytynyt suoraa sovellettavia tutkimustuloksia.

Hankkeen aikana tämä olettamus tutkimuksen ja kehittämistyön ajankohtaisesta ja tarpeellisuudesta vahvistui. Usea organisaatio otti projektioppaan käyttöön jo luonnosvaiheessa, koska muuta ei ollut käytössä. Projektimallin rakenne otettiin välittömästi käyttöön kolmessa merkittävässä yhteishankkeessa, yli neljässäkymmenessä valtionhallinnon organisaatiossa. Osassa näissä organisaatioissa on paljon eroja mm. henkilöstömäärän ja toiminnan osalta.

Projektimallin pohjalta pystyttiin suunnittelemaan ohjeisto- ja työkalukokonaisuus. Kokonaisuudessa hyödynnettiin projektimallin kirjain- ja numeroyhdistelmää. Valtion IT-palvelukeskus ylläpitää koordinoimilleen yhteishankkeille ns. työkalupakkia, joka sisältää projektimallin, -projektioppaan ja näiden mukaan tehtyjä työkaluja.

4.1 Projektimallin rakenne

Projektimalli jakaa tietoturvallisuuden hallinnan sellaisiin kokonaisuuksiin, joissa organisaation mahdollista suunnitella ja toteuttaa kokonaisuus aikaisempaa hallitummin. Projektimallin rakennetta hyödynnettiin projektioppaan laatimisessa (ks. liite 1).

Projektimallin osa-aluejaon ja numeroinnin avulla kuhunkin osaan on mahdollista liittää ohjeistoja, dokumenttipohjia ja erilaisia työkaluja. Projektimallin pohjalta suunniteltiin ohjeistorakenne (kuvio 9).

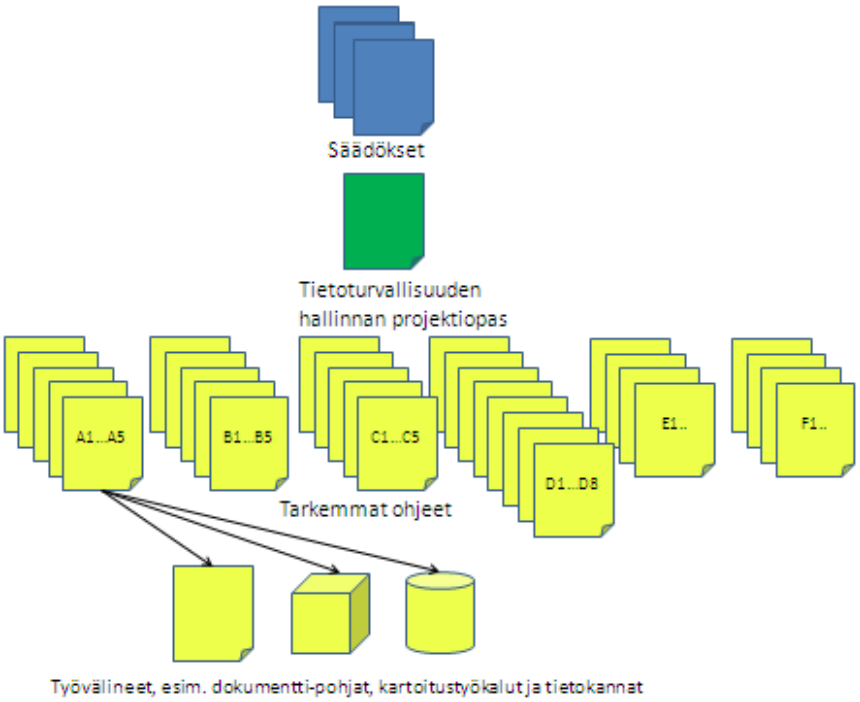
Koska eri vaiheet on indeksoitu kirjaimella sekä numerolla, voidaan niihin liittää tarkempia ohjeita sekä työvälineitä. Esimerkiksi tietoturvallisuusasetuksen täytäntöönpanon yhteishankkeessa osa-alueeseen A laadittiin seuraavat työvälineet:
A1 Yhteenveto tietoturvallisuuden vaatimuksista (ohje ja dokumenttipohja)
A1 Tietoturvatavoitteiden määrittäminen (ohje ja dokumenttipohja)
A1 Tietoturvallisuuden hallinnan kattavuuden määrittäminen (ohje ja dokumenttipohja)
A1 Tavoitteiden ja vaatimusten kohdentaminen (ohje ja taulukkopohja)
A2 Tietoturvatavoitteiden määrittäminen (ohje ja lomakepohja)
A3 Tietoturvallisuuden hallinnan roolit (ohje ja dokumenttipohja)
A4 Projektin vaiheistus (ohje ja dokumenttipohja)
A4 Projektin organisointi (ohje ja dokumenttipohja)

A4 Projektisuunnitelma (ohje ja dokumenttipohja)
A5 Johdon hyväksynnän ja tuen hankkiminen (ohje ja dokumenttipohja)

Vastaavalla tavalla jokaiseen osa-alueeseen on laadittu tarkempia ohjeita ja työvälineitä. Koska edellä luetellut tarkemmat ohjeet ja dokumenttipohjat on laadittu valtiovarainministeriön yhteishankkeen yhteydessä, ne eivät ole julkisesti saatavilla. Sen vuoksi perustettiin Internet www.tietoturvatalkoot.fi. Sivuston tarkoituksena on koota vastaavalla tavalla eri osiin sekä tehtäviin liittyviä työkaluja vapaaehtoisvoimin. Kaikki sivustolle materiaalia tuottavien nimet näkyvät työvälineiden käyttäjille. Sivusto on vielä marraskuussa 2011 vasta perustamisvaiheessa.

4.2 Projektimallin soveltamisalue ja jatkokehityskohteet

Projektimallia voidaan pienin muutoksin soveltaa valtionhallinnon lisäksi yksityisellä sektorilla. Tämä tulisi kuitenkin testata ja tarkastella erikseen. Tärkein soveltamisalue on mahdollisuus tehdä opasta täydentäviä dokumentteja sekä työkaluja. Kuviossa 8 on esitetty, miten kirjain- ja numeroyhdistelmillä voidaan yksilöidä eri osa-alueiden työvälineet. Näin eri tehtäviin löytyy tukea aikaisempaa helpommin. Kuviossa on esimerkkinä tehtävä C1, eli ”Riskienhallinta- ja häiriötilannemenettelyjen määrittäminen sekä kuvaaminen”. Kuviossa alhaalla esitetyt työvälineet voivat olla esimerkiksi riskikartoitustyökaluja, kartoituslomakkeita ja riskienhallintatietokantoja.



Kuvio 9. Luonnos ohjeistokokonaisuudesta.

4.3 Projektiopas

Projektioppaan tehtävänä oli opastaa käytännönläheisesti toteuttamaan tietoturvallisuuden hallintajärjestelmä vaihe vaiheelta. Oppaan on yhteensopiva ainakin tietoturvallisuusasetuksen (TTA 681/2010), VAHTI 2/2010 liitteen 5 tietoturvatasovaatimusten sekä KATAKRIn (Kansallinen auditointikriteeristö, 2009) kanssa. Yhteensopivuudella varmistetaan, että se tukee eri vaatimusten toteuttamista, mutta ei kuitenkaan tee tietoturvallisuuden hallintakokonaisuudesta liian jäykkää. Projektiopas on tämän raportin liitteenä 1.

Vaiheet, tehtävät ja erimerkeiksi tarkoitetut lopputulokset on esitetty projektimallin mukaisessa järjestyksessä projektimallia (ks. liite 1):
Osa-alue A Tietoturvatarpeiden ja lähtökohtien tunnistaminen
Osa-alue B Tärkeiden toimintojen, riippuvuuksien ja tieto-omaisuuden tunnistaminen
Osa-alue C Riskienhallinta- ja häiriötilannemenettelyiden luominen
Osa-alue D Tietoturvallisuuden hallintamenettelyjen luominen

Täydentävät osat

Osa-alue E Tietoturvallisuuden fyysiset ja tekniset järjestelyt
Osa-alue F Ennalta ehkäisevä toiminta, toiminnan varmistaminen ja jatkuva kehittäminen

Liitteet

Liite 1 Oppaan tehtävien liittyminen VAHTI 2/2010 liitteen 5 tietoturvatasojen kriteereihin
Liite 2 Oppaan tehtävien liittyminen KATAKRIin (vuoden 2009 versio)
Liite 3 Oppaan liittyminen asetukseen tietoturvallisuudesta valtionhallinnossa

Liitteissä 1-3 on esitetty, miten lähteen eri kohdat liittyvät projektimalliin. Näin lukija voi etsiä oppaasta suoraan sen kohdan, josta haluaa lisätietoja. Projektioppaasta on laadittu ulkoasullisesti kaksi versiota. Toinen versioista on tarkoitettu sähköisesti jaettavaksi ja toinen versio on tämän raportin liitteenä. Jälkimmäinen on tehty Laurean opinnäytetyöohjeen mukaiseen muotoon.

4.4 Projektioppaan soveltamisalue ja kehitys

Projektiopasta voidaan soveltaa valtionhallintoa laajemmin. Siitä on suunnitteilla yksityiselle sektorille suunnattu versio 2.0. Uudessa versiossa huomioidaan myös KATAKRI:n uudempi ver-

sio sekä ISO/IEC 27001 –standardi (laaditaan vastaavuustaulukko oppaan loppuun). Oppaaseen tulee lisäksi täydennyksiä erityisesti osa-alueisiin E ja F.

4.5 Tietoturvakäsikirja

Kun projektimallia ja –opasta sovellettiin tutkimuksen implementointivaiheessa eräässä ministeriössä, syntyi tietoturvallisuuden hallintakokonaisuuden kuvaava tietoturvakäsikirja. Käsikirjasta laadittiin dokumenttipohja, joka on tietoturvallisuusasetuksen toimeenpanon yhteishankkeen organisaatioiden hyödynnettävissä. Käytännössä käsikirjapohjaa voidaan hyödyntää laajemmin valtionhallinnossa. Käsikirjan lopussa on liite, jossa on esitetty, missä käsikirjan kohdassa kukin tietoturvatasovaatimus on käsitelty vähintään perustasolla (ks. taulukko 1).

1.1. Johtajuudelle asetettavat vaatimukset		
1.1.1 Strateginen ohjaus		Käsikirjan asiaa käsittelevä kohta
1.1.1.1. Perustaso	Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.	luku 2
1.1.1.2. Perustaso	Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.	luku 8
1.1.1.3. Perustaso	Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.	luku 2
1.1.1.4. Korotettu taso	Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.	luku 2.5
1.1.1.5. Korkea taso	*Organisaatiolla on vuosittainen tietoturvallisuuden kehittämissuunnitelma.*	luku 6.2
1.1.1.6. Korkea taso	*Tulosohjauksessa käytetään myös tietoturvallisuuteen liittyviä osuuksia.*	luku 2, luku 6.1

Taulukko 5 Esimerkki tietoturvakäsikirjan liitteestä 2.

Tietoturvakäsikirjan liitteessä 2 olevaa taulukkoa hyödyntävät sekä tietoturvallisuuden kehittämiseen osallistuvat, että auditoijat. Auditoija näkee taulukosta suoraan, missä kohdassa auditoitavaa vaatimusta käsitellään. Taulukkoa hyödynnettiin mm. Arkistolaitoksen kohdeorganisaatiolle teettämässä Sähke2 –auditoinnissa.

5 Työn arviointi

Konstruktiivisen tutkimuksen tavoitteena on saada käytännön ongelmaan uudenlainen ja teoreettisesti perusteltu ratkaisu, joka tuo uutta tietoa. Tutkimuksessa on oleellista sitoa käytännön ongelma ja sen ratkaisu teoreettiseen tietoon. Lisäksi ratkaisu tulee voida osoittaa toimivaksi. Ojasalon ja kumppanien mukaan opinnäytetyössä ja muissa kehittämistöissä joudutaan usein pohtimaan, miten selvä näyttö rakenteen toimivuudesta tarvitaan. (Ojasalo jne.). Tässä kehittämistyössä ei pystytty kokoamaan selvää näyttöä rakenteen toimivuudesta, sillä monella projektimallia ja –opasta soveltavalla organisaatiolla tietoturvallisuuden kehittämistyö on vielä kesken. Mikäli kehittämishanke olisi jatkunut vuoden 2013 loppuun, tilanne olisi todennäköisesti toinen.

5.1 Kehittämisprojektin arviointi

Tämän kehittämisprojektin onnistumiseen vaikutti merkittävästi oikea-aikaisuus ja omat työtehtävät Valtion IT-palvelukeskuksessa sekä valtiovarainministeriössä. Mikäli projektimallin suunnittelun alkuvaiheessa ei olisi ollut käynnissä kuuden organisaation kehittämishanketta, palautteen saaminen olisi ollut haastavampaa. Kehittämishanke mahdollisti sen, että sen hetkiset kehittämistulokset saatiin heti kokeiltavaksi käytännön työssä.

Kehittämistulokset otettiin tarkemmalla tasolla käyttöön valtiovarainministeriössä kevään 2011 alusta lähtien. Siellä projektimallia ja –opasta oli mahdollista kokeilla käytännön tietoturvallisuuden kehittämistyössä. Konkreettisena osoituksena projektimallin- ja oppaan soveltamisesta syntyi valtiovarainministeriön tietoturvakäsikirja.

Kehittämistyön käytännön soveltaminen laajeni kevään 2011 aikana. Tuolloin käynnistyi ensimmäinen neljästä tietoturvallisuusasetuksen toimeenpanon yhteishankkeesta. Näihin on ilmoittautunut mukaan yli viisikymmentä valtionhallinnon organisaatiota. Mikäli tällaisia hankkeita ei olisi käynnistynyt, olisi käytännön soveltaminen ainakin alussa jäänyt vähäisemmäksi. Yhteishankkeiden kokemusten ja palautteen perusteella projektimallia ja –opasta voidaan jatkossa kehittää edelleen.

5.2 Validiteetti, reliabiliteetti ja vakuuttavuus

Tämän kehittämistyön tuloksia oli tarkoitus arvioida sen mukaan;

1. Miten ne ovat sovellettavissa yleisesti valtionhallinnossa ja miten ne otetaan vastaan käyttäjäkunnassa;
2. Voidaanko niiden perusteella suunnitella ja toteuttaa tietoturvallisuuden hallintajärjestelmä niin, että se toteuttaa vähintään edellä kuvatut vaatimukset;

3. Miten kehittämistuloksia voidaan kehittää edelleen.

Kehittämishankkeen aikana sekä projektimalli, että projektiopas otettiin suoran käyttöön yli 20 organisaatiossa. Koska kaikkien organisaatioiden tietoturvallisuuden kehittämistyö on edelleen kesken, kehittämistyötä on vaikea arvioida luotettavasti. Valtiovarainministeriön tietoturvallisuuden kehittämishanke osoitti, että projektimallin ja –oppaan avulla voidaan tehokkaasti kehittää tietoturvallisuuden hallintaa. Tehokkuudesta yksi konkreettinen näyttö oli tietoturvakäsikirja, jossa on kuvattu tietoturvallisuudenhallintakokonaisuus merkittävine turvakontrolleineen.

Projektimallin ja –oppaan yleisyys valtionhallinnon tasolla on vielä vähäistä. Tätä raporttia kirjoitettaessa molemmat on otettu ainakin osittain käyttöön lähes viidessäkymmenessä valtinhallinnon organisaatiossa, määrä kasvaa koko ajan mm. yhteishankkeiden ja tietoisuuden kasvamisen myötä. Kiinnostuksesta kertoo mm. sähköpostitse ja puhelimitse tapahtuneet yhteydenotot eri valtionhallinnon organisaatioista.

Projektimallin ja –oppaan helppokäyttöisyyttä ei tässä tutkimuksessa erikseen käsitelty. Käyttäjät antoivat kuitenkin palautetta kehittämishankkeen aikana. Projektiopasta kehitettiin annetun palautteen perusteella.

Projektimallia ja -opasta kommentoitiin kolmen yksityisen sektorin asiantuntijoiden toimesta. Kaikkien kommentoijien mielestä sekä projektimalli- että opas on pienellä kehittämisellä laajennettavissa yksityiselle sektorille. Tämän lisäksi haastattelin Valtion IT-palveluiden kahta yhteishankkeista vastaavaa asiantuntijaa. Projektimallin arvosanat 4,5 ja 4,5. Projektioppaan soveltuvuus yhteishankkeisiin 4 (koko valtionhallinto) 5 (valtioneuvostoasiakkaat). Arvioinnissa ei selvitetty, miltä laajuudelta projektimalli otettiin niissä organisaatioissa käyttöön, jotka ilmoitti näin tekevänsä. Arvosanan antaneita organisaatioita oli ainoastaan 5 kpl. Näin pienen otannan perusteella ei voida muodostaa luotettavaa näkemystä työn laadusta. Tämän lisäksi arvosanan käyttö laadulliseen arviointiin on ainoastaan suuntaa antava. Luotettavampi arviointi olisi tapahtunut laajemmalla otannalla, esimerkiksi teemahaastatteluin.

Jatkossa projektimallin ja –oppaan toimivuutta voitaisiin arvioida esimerkiksi Marchin ja Smithin mukaan metodin arviointiperusteilla:

1. kyky suorittaa aiottu tehtävä,
2. tehokkuus,
3. yleisyys ja
4. helppokäyttöisyys. (Järvinen & Järvinen 2004)

Näihin arviointikriteereihin voidaan liittää useita kysymyksiä niin kehittämishankkeesta, kuin tietoturvallisuuden jatkuvasta kehittämisestä.

5.3 Mahdollisuudet

Projektimalli mahdollistaa laajan, rakenteistetun ohjeistokokonaisuuden luomisen. Tällainen on otettu käyttöön jo Valtion IT-palvelukeskuksen asiakkaita palvelevassa ”työkalupakissa”. Interet –sivustolla www.tietoturvatalkoot.fi on kehitteillä vapaaehtoisvoimin tehtävä tietoturvasivusto. Sivusto hyödyntää projektimallin rakennetta. Samanlainen ohjeisto- ja työkalukokonaisuus on mahdollista toteuttaa myös laajempaan käyttöön. Dynaamisen tietoturvallisuuden hallinnan malli ja –opas voidaan myös tuottaa palveluna. Sitä voidaan myös hyödyntää laajemmin erilaisissa yhteistyöhankkeissa. Projektimalli ja –opas voidaan lisäksi laajentaa käsittämään kokonaisturvallisuutta, jolloin kokonaisuus käsittelisi dynaamista turvallisuuden hallintamallia ja –opasta.

6 Yhteenveto

Tietoturvallisuuden merkitys yhteiskunnassa kasvaa. Osa valtionhallinnon organisaatioista panostavaa tietoturvallisuuden kehittämiseen oma-aloitteisesti, toiset organisaatiot tarvitsevat kehittämistyöhön ulkoista painetta. Asetus tietoturvallisuudesta valtionhallinnossa (TTA 681/2010) auttaa organisaation tietoturvallisuudesta vastaavaa perustelemaan tietoturvallisuuden kehittämistyötä omassa organisaatiossa.

Tietoturvallisuuden kehittämistyö on haastavaa. Se vaatii teknistä ja hallinnallista osaamista, kokonaisuuksien hallintaa ja määrätietoisuutta. Osallistuessani vuosien ajan valtionhallinnon organisaatioiden tietoturvallisuuden kehittämishankkeisiin, olen havainnut, että usein tietoturvallisuudesta vastaavan työ on varsin yksinäistä. Valtionhallinnon organisaation tietoturvavastaava voi kuitenkin tehdä yhteistyötä toisten organisaatioiden tietoturvallisuudesta vastaavien kanssa. Tästä hyvänä esimerkkinä toimivat valtionhallinnossa käynnissä olevat tietoturvallisuuden kehittämisen yhteishankkeet. Näissä hankkeissa pyörää ei keksitä uudelleen, vaan kootaan olemassa olevia hyviä käytänteitä jalostettavaksi. Projektimalli- ja opas auttavat tässä hallitsemaan kokonaisuutta ja ohjaamaan varsinaista kehittämistyötä. Projektimallin- ja oppaan avulla organisaatio pystyy keskittymään olennaiseen sen sijasta, että etsii tietotulvasta omassa organisaatiossa käyttökelpoiset asiat ja kamppailee suuren työmäärän priorisoinnin kanssa.

Se, täyttääkö organisaatio tietoturvallisuuden ns. perustason ja mahdollisesti sitä korkeampia tasoja on viime kädessä kiinni organisaatiosta itsestään. Ohjeiden, työkalujen ja tuen merkitys jää pieneksi, mikäli organisaatio – varsinkaan sen johto, ei sitoudu ja osoita resursseja tietoturvallisuuden kehittämistyölle. Usein tällainen sitoutuminen vaatii vähintään yhtä sellaista henkilöä, joka ottaa asiakseen perustella kehittämistarpeet ja ottaa vastuun asian edistämisestä. Projektioppaan tehtävänä on tukea tässä työssä.

Projektimalli- ja opas ovat saaneet hyvän vastaanoton valtionhallinnossa. Sen vuoksi tullaan niitä kehittämään jatkossa. Se jää nähtäväksi, kehitetäänkö ensin kokonaisuutta kattamaan turvallisuuden hallintaa laajemmin, vai muokataanko projektioppaasta yksityiselle sektorille suunnattu versio.

Lähteet

Kuula, A. K. 1999. Toimintatutkimus, Kenttätyötä ja muutospyrkimyksiä. Tampere: Vastapaino.

ISO/IEC TR 13335-3:1998. Guidelines for the management of IT Security - Part 3: Techniques for the management of IT. Geneva: Security International organization for standardization.

ISO/IEC TR 13335-4:2000. Guidelines for the management of IT Security - Part 4: Selection of safeguards. Geneva: International organization for standardization.

ISO/IEC TR 13335-5:2001. Guidelines for the management of IT Security - Part 5: Management guidance on network security. Geneva: International organization for standardization.

ISO/IEC 27001:2005. Information security management systems – Requirements. International organization for standardization.

ISO/IEC 27000:2009. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27001:2005, Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27002:2005, Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27003:2010, Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27004:2009, Tietoturvallisuuden hallinta. Mittaaminen. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27005:2008, Tietoturvariskien hallinta. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27006:2007, Tietoturvallisuuden hallintajärjestelmien auditointi- ja sertifiointielinten vaatimukset. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27007, Tietoturvallisuuden hallintajärjestelmän auditointiohjeet.

Kallioinen, O. 2008. Oppiminen Learning by Developing –toimintamallissa. Laurea-ammattikorkeakoulu.

Kansallinen turva-auditointikriteeristö (KATAKRI), 2009. Puolustusministeriö. (Saatavana osoitteesta www.defmin.fi.)

Kuusela. Realistinen toimintatutkimus? Toimintatutkimus, työorganisaatiot ja realismi. Helsinki:2005

Ojasalo, K., Moilanen, T. & Ritalahti J. 2009. Kehittämistyön menetelmät - uudenlaista osaamista liiketoimintaan. Helsinki: WSOY pro.

Petri Puhakainen. 2006. A Design Theory for Information Security Awareness, Oulun yliopisto.

Valtiovarainministeriö. 2007. Valtionhallinnon tietoturvatasot, hankeryhmän loppuraportti. (Saavavana osoitteesta www.valtiovarainministeriö.fi)

Valtiovarainministeriö. 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010.

Valtiovarainministeriö. 2007. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan VAHTI 3/2007

Sähköiset lähteet

Arkistolaki (831/1994) 7§, 8§, 4. luku. Tulostettu 20.10.2010

Asetus tietoturvallisuudesta valtionhallinnossa (TTA, 681/2010) Tulostettu 16.8.2010

Asetus viranomaisten toiminnan julkisuudesta (1030/1999) Tulostettu 19.10.2010

Henkilötietolaki (523/1999) Tulostettu 20.10.2010

Laki turvallisuusselvityksistä (177/2002) Tulostettu 21.10.2010

Laki viranomaisten toiminnan julkisuudesta (621/1999) ja 38§:n muutos (636/2000) Tulostettu 19.10.2010

Suomen perustuslaki (731/1999) -10§ ja 12§. Tulostettu 19.10.2010

Sähköisen viestinnän tietosuojalaki (516/2004) Tulostettu 21.10.2010

Valmiuslaki (1080/1991) Tulostettu 21.10.2010

http://www.huolintaliitto.fi/ytnk08/fi/julkaisut_liitteet/KATAKRI_suositusohje_lopullinen.pdf Kansallisen turvallisuusauditointikriteeristön (KATAKRI) suositusosuuden käyttöohje

Valtiovarainministeriö. Keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004) Tulostettu 15.11.2010

Valtiovarainministeriö. Tietoturvallisuuden arviointi valtionhallinnossa (VAHTI 8/2006) Tulostettu 20.11.2010

Valtiovarainministeriö. Tietoturvallisuuden hallintajärjestelmän arviointisuositus (VAHTI 3/2003) Tulostettu 15.11.2010

Valtiovarainministeriö. Tietoturvallisuus ja tulosohjaus (VAHTI 2/2004). Tulostettu 15.11.2010

Valtiovarainministeriö. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä, VAHTI 7/2009. Tulostettu 20.10.2010

Valtiovarainministeriö. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, VM 0024:00/02/99/1998 Tulostettu 20.10.2010

VATT http://www.vatt.fi/file/vatt_publication_pdf/t159.pdf Mainettaan parempi tuottavuusohjelma? Katsaus valtion virastojen ja laitosten työn tuottavuuteen ja työhyvinvointiin

www.google.com. Hakutulos sanoilla ”tietoturvallisuuden hallinta”. Tulostettu 4.5.2011

www.google.com. Hakutulos sanoilla ”information security management”. Tulostettu 4.5.2011

Tanskan valtionhallinnossa kehitetty tietoturvastandardi http://www.itst.dk/sikkerhed/standarder/ds-484-og-iso-27002/kapitler-i-ds-484 (Poimittu 23.5.2011)

Kuviot

Taulukot

Liitteet

Liite 1
Laurea-ammattikorkeakoulu
Leppävaara

Tietoturvallisuuden hallinnan suunnittelu ja toteutus
Projektimalli ja – opas valtionhallintoon

Kirsi Nurmi
Turvallisuusosaamisen ko.
Opinnäytetyö
Marraskuu, 2011

Sisällys

Lukijalle

Tämä opas on suunnattu tietoturvallisuuden kehittämiseen osallistuville asiantuntijoille. Vaikka kyseessä on projektiopas, en käy läpi projektien perusasioita, vaan käsittelen tietoturvallisuuden hallintaa niin, että suuri työmäärä saadaan jaettua helpommin hallittaviin kokonaisuuksiin.

Monet tässä oppaassa olevat tehtäväsisällöt pohjautuvat niihin ajatuksiin, mitä on syntynyt tehdessäni yhteistyötä muiden asiantuntijoiden kanssa. Lista näistä henkilöistä on pitkä. Kahden vuoden sisällä minulla on ollut ilo työskennellä kahdessa loistavassa tiimissä. Kiitos Ulkoasiainhallinnon TOPA-tiimille Antti Savolaiselle, Kari Pohjolalle, Jukka Nyblomille, Jaakko Oksaselle ja Mikko Mutkalle. Kiitos myös Kimmo Rouskun johtamalle Valtion IT-palvelukeskuksen tietoturvatiimille ja valtiovarainministeriön Irja Peltoselle. Lämmin kiitos myös tätä opasta työvaiheessa kommentoineille.

Hyvä lukija, toivotan Sinulle onnea kehittämistyöhön. Iloitse pienestäkin kehityksestä, sillä se on askel oikeaan suuntaan!

Järvenpäässä 11.11.2011

Kirsi Nurmi

Johdanto

Tämä opas on tarkoitettu niille, jotka kehittävät organisaationsa tietoturvallisuuden hallintaa. Oppaan tarkoituksena on jakaa tietoturvallisuuden kehittäminen sellaisiin tehtäviin ja lopputuloksiin, joita on mahdollisimman helppo projektoida ja myöhemmin ylläpitää. Tehtäviä voidaan toteuttaa samanaikaisesti ja esitetty järjestys on tarkoitettu suunniteltavaksi organisaation omista lähtökohdista.

Opas huomioi asetuksen tietoturvallisuudesta valtionhallinnossa, KATAKRIn ja VAHTI 2/2010 liitteen 5 tietoturvavaatimukset. Mikäli opasta on tarkoitus soveltaa projektissa, jossa toteutetaan VAHTI 2/2010 liitteen 5 tietoturvatasoja, on suositeltava tutustua liitteeseen 1. Taulukossa esitetään, mitkä vaatimukset liittyvät tämän oppaan tehtäviin A1-D8. Liitteessä 2 on vastaavasti käsitelty KATAKRIn kriteerien liittyminen eri tehtäviin. Oppaan vastaavuutta tietoturva-asetukseen on käsitelty liitteessä 3.

Kriteeristöstä tai viitekehyksestä riippumatta on suositeltava laatia soveltamissuunnitelma, jossa vaiheistetaan eri tehtävät. Soveltamissuunnitelmaa on käsitelty tehtävässä C5.

Oppaasta voidaan tarvittaessa poimia pelkästään kiinnostavimmat kohdat. Jokaisen tehtäväalueen otsikon alta löytyy taulukko, jossa on kuvattu vaiheen tärkeimmät tehtävät ja lopputulokset. Yhteenveto oppaan osa-alueista tehtävineen on kuvattu liitteessä 1.

Alla on esimerkki tehtävän A4 taulukosta.

Tehtävät • Projektisuunnitelman laatiminen tietoturvallisuuden hallinnan kehittämiseen. • Projektiorganisaation muodostaminen. Vaiheen lopputulokset • Projektisuunnitelma (johto hyväksyy). • Projektiorganisaatio.

Projektimallissa tärkeimmät vaiheet on jaettu neljään erilaisista tehtävistä koostuvaan osaan (A-D). Jokainen tehtävä lopputuloksineen ja esimerkkeineen on tarkoitettu sovellettavaksi organisaation omien tarpeiden mukaan.

Osa-alue A Tietoturvatarpeiden ja lähtökohtien tunnistaminen
Osa-alue B Tärkeiden toimintojen, riippuvuuksien ja tieto-omaisuuden tunnistaminen
Osa-alue C Riskienhallinta- ja häiriötilannemenettelyiden luominen
Osa-alue D Tietoturvallisuuden hallintamenettelyjen luominen

Täydentävät osat

Osa-alue E Tietoturvallisuuden fyysiset ja tekniset järjestelyt
Osa-alue F Ennalta ehkäisevä toiminta, toiminnan varmistaminen ja jatkuva kehittäminen
Liite 1 Oppaan tehtävien liittyminen VAHTI 2/2010 liitteen 5 tietoturvatasojen kriteereihin
Liite 2 Oppaan tehtävien liittyminen KATAKRIin
Liite 3 Oppaan liittyminen asetukseen tietoturvallisuudesta valtionhallinnossa

Sanasto

Tässä sanastossa on lyhyesti kuvattu oppaassa käytettyjä avainsanoja. Valtiovarainministeriö ylläpitää kattavampaa ja laajasti käytössä olevaa tietoturvasanastoa valtionhallinnolle (VAHTI 8/2008).

Erityistilanne

Normaalista poikkeavaa johtamismallia ja viestintää vaativa tilanne.

Häiriötilanne

Tilanne, jossa toiminta on hankaloitunut tai vaarantunut. Tietoturvallisuuden häiriötilanteita kutsutaan myös ”tietoturvapoikkeamatilanteiksi”. Häiriötilanteita voi olla sekä normaali- että poikkeusoloissa.

KATAKRI

Kansallinen auditointikriteeristö. Sillä kaksi päätehtävää:

1) yhtenäistää viranomaisten tekemät tarkastus- ja auditointikriteerit
2) organisaatiot käyttävät tätä neliportaista kriteeristöä turvallisuustason määrittämisessä.

http://www.defmin.fi/files/1525/Katakri.pdf

Normaaliolot

Olosuhteet, joissa sovelletaan normaaliolojen lainsäädäntöä (vrt. poikkeusolot).

VAHTI 2/2010

Valtionhallinnon tietoturvallisuuden johtoryhmän laatima ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta”. Ohjeen tehtävänä on auttaa organisaatioita 1.10.2010 voimaan tulleen tietoturvallisuusasetuksen (681/2010) täytäntöönpanossa.

Poikkeusolot

Valmiuslaissa (1080/1991) määritetty tila.

Soveltamissuunnitelma

Dokumentti, jossa kuvataan, miten tietyn kriteeristön tai lähteen vaatimukset huomioidaan omassa toiminnassa.

Tietoturvatasot

VAHTI 2/2010 liitteessä 5 kuvatut tietoturvakriteerit (vrt. KATAKRI).

Turvallisuusluokitus/tietoturvaluokitus

Turvallisuuden tai tietoturvallisuuden näkökulmasta tehty luokitus. Esim. luottamuksellisuuden mukaan, suojausvaatimusten tai turvallisuuskriteerin mukaan.

Tuki tietoturvallisuudesta vastaavan työlle

Työn projektointi

Tietoturvallisuuden hallintakokonaisuuden rakentaminen ja ylläpito vaatii paljon työtä. Ilman selkeitä tavoitteita, riittäviä resursseja ja ohjausta työmäärä voi käydä ylivoimaiseksi. Projektointi on keino hallita kokonaisuutta. Se voi myös helpottaa yhteistyön tekemistä eri toimijoiden kesken, koska projekti ylittää normaalit linjaorganisaation rajat. Projektin aikana syntyneitä verkostoja voi käyttää myöhemmin hyväksi tietoturvallisuuden kehittämisessä.

Yhteistyö muiden organisaatioiden kanssa

Tietoturvatyöhön varataan harvoin riittävästi työvoimaa. Valtion tuottavuusohjelman vuoksi henkilöstöltä odotetaan tehokkuutta ja kehittäminen tehdään usein oman työn ohessa. Valtionhallinnossa tietoturvallisuuden hallinnan pääperiaatteet ovat kuitenkin saman luonteisia, sen vuoksi on suositeltava verkostoitua muiden tietoturva-asiantuntijoiden kanssa.

Tietoturvallisuuteen liittyvää opastusta saa viranomaisilta, kuten Viestintävirastosta ja tietosuojavaltuutetun toimistosta. Tämän lisäksi Valtion IT-palvelukeskus ylläpitää asiakkailleen tietoturvallisuuden työkalupakkia. Siellä löytyy esimerkiksi tähän oppaaseen liittyvää tukimateriaalia. Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) ylläpitää kattavaa tietoturvallisuuden ohjeistusta Valtiovarainministeriön internet –sivustolla http://www.vm.fi.

Tietoturvakäsikirja

Tietoturvallisuuden hallintaan liittyy paljon säännöllisesti ylläpidettävää dokumentaatiota, sen vuoksi kokonaisuus kannattaa suunnitella huolella. Tässä oppaassa suositellaan tietoturvakäsikirjan laatimista oman työn ja tietoturvallisuuden ohjauksen tueksi. Tietoturvakäsikirjassa kuvataan, miten tietoturvallisuutta hallitaan ja mistä eri dokumentit löytyvät. Tietoturvakäsikirjan avulla on helpompi perehdyttää muita tietoturvatyöhön osallistuvia, kuten varahenkilöitä. Käsikirjan laatimista on käsitelty tehtävässä D5.

Oma henkilöstö

Alussa tietoturvallisuuden hallinta on usein ”tulipalojen sammuttamista” ja varsinaiseen kehittämistyöhön jää vähän aikaa. Vaikka tietoturvaperiaatteet ja ohjeet alkuvaiheessa puuttuisivat, on tärkeää että henkilöstö osaa tarvittaessa kysyä neuvoa tai vähintään ilmoittaa, kun havaitaan potentiaalisia ongelmia.

Johdon tuki

Johdon tuki on tietoturvatyön onnistumisen kannalta elintärkeää. Tietoturvatyö ei välttämättä vaadi paljoa aikaa johdolta, jos se on luonteva osa muuta työskentelyä ja kokouskäytäntöjä. Käytännössä tuki voi olla sitä, että johdon edustajat osoittavat tukeaan esim. puhumalla tietoturvallisuuden tärkeydestä henkilöstölle, ovat esimerkkinä muille ja käsittelevät tietoturvallisuusasiat vähintään puolivuosittain tietoturvallisuuden ohjausryhmässä.

Viestintä

Normaalitoiminnassa tietoturvaviestintään soveltuvat usein organisaation tavanomaiset viestintäkanavat. Erityistilanteita varten on lisäksi syytä suunnitella tehostetun viestinnän menettelyt. Suunnittelussa voidaan tehdä yhteistyötä organisaation viestinnästä vastaavien kanssa. Alkuvaiheessa tulisi varmistaa, että henkilöstö ja muut tarvittavat sidosryhmät saavat riittävän hyvin tietoa ainakin päivitetyistä yhteystiedoista, tietoturvaohjeista ja –käytännöistä.

Työn aloittaminen

Tietoturvallisuuden hallintaprojektin tarkoituksena on luoda kokonaisuus, jolla tietoturvallisuutta hallitaan ja kehitetään. Projektissa kerätään tietoa organisaatiosta, luodaan menettelytapoja tietoturvallisuuden hallintaan ja suunnitellaan jatkokehitystoimet. Jos tietoturvallisuuden hallintaan sisältyy tiettyjen kriteeristöjen tai vaatimuslähteiden täyttäminen, voidaan ennen projektin aloittamista tarkastaa, miten hyvin organisaatio täyttää kriteerit.

Vaatimuslähteiden ja kriteerien ei kuitenkaan tulisi liikaa ohjata varsinaista tietoturvallisuuden hallintakokonaisuuden suunnittelua ja toteutusta. Esimerkiksi tietoturvallisuuden hallintajärjestelmää ei tule toteuttaa kriteeristön mukaan numerojärjestyksessä vaan toteuttamista varten kannattaa laatia organisaation omiin tarpeisiin perustuva projektisuunnitelma.

Vaatimus	**Toteutuminen organisaatiossa**	**Vastuu**	**Vaatimuksen toteutumisen tila**

Taulukko 6 Tiettyyn kriteeristöön tapahtuva arviointi voidaan tehdä esimerkiksi tällaisella taulukolla.

Kuntaliiton projektioppaassa ”Onnistunut projekti” esitellään keinoja projektien onnistuneeseen läpivientiin. Opas on ladattavissa Internet-osoitteessa http://hosted.kuntaliitto.fi/intra/julkaisut/pdf/p071005095633P.pdf .

Seuraavalta sivulta lähtien on esitetty tässä oppaassa käsiteltävät tehtävät. Tehtävät on tarkoitettu avuksi kokonaisuuden hallintaan ja hanke-/projektisuunnitteluun. Eri tehtäviä voi toteuttaa samanaikaisesti. Numeroinnit ja järjestys ovat suuntaa antavat. Organisaation tulee suunnitella kokonaisuus omista lähtökohdistaan. Oppaan lopussa on kolme liitettä, joissa on kuvattu eri tehtävien liittyminen VAHTI 2/2010 tietoturvatasovaatimuksiin, KATAKRIin ja tietoturvallisuusasetukseen.

1.1. Johtajuudelle asetettavat vaatimukset		
1.1.1 Strateginen ohjaus		Tehtävä
1.1.1.1. Perustaso	Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.	A1, A3, D5, D6
1.1.1.2. Perustaso	Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.	A3, B2

Taulukko 7 Esimerkki oppaan tehtävien liittymisestä VAHTI 2/2010 tietoturvatasovaatimuksiin.

Tunnus		Kriteerin pääasiallinen sisältö	Tehtävä
A	101	Johdon tukema ja tarkistama turvallisuuspolitiikka	B5, D7
A	102	Turvallisuuspolitiikan ja/tai turvallisuuden johtamisen riittävän kattavuuden varmistaminen turvallisuusdokumentaatiossa	A2, B1, B3, B4, C5, D2
A	103	Turvallisuusdokumentaation vastaavuus organisaation riskeihin nähden	B3, B5, C1, C2, C3, C4, D1, D2, D3, D5, D6, D7, D8

Taulukko 8 Esimerkki oppaan tehtävien liittymisestä KATAKRIn vuoden 2009 versioon.

A Tietoturvatarpeiden ja lähtökohtien tunnistaminen
A1 Tietoturvallisuuden lähtökohtien määrittäminen ja kuvaaminen Tärkeimmät tehtävät ➢ Tunnistetaan toimintaan kohdistuvat erityisvaatimukset. ➢ Esitellään tärkeimmät tietoturvavaatimukset johdolle. ➢ Määritellään tietoturvatavoitteet. ➢ Suunnitellaan, miten vaatimukset ja tavoitteet kohdistetaan organisaatiossa. ➢ Valitaan/suunnitellaan tietoturvaluokittelu. Tärkeimmät lopputulokset ➢ Lyhyt yhteenveto tietoturvallisuuden kannalta merkittävistä vaatimuksista. ➢ Kuvaus organisaation tietoturvatavoitteista. ➢ Suunnitelma tietoturvavaatimusten ja tavoitteiden kohdistamisesta. ➢ Kuvaus tietoturvaluokittelusta.
A2 Alustava tietoturvallisuuden hallinnan kattavuuden määrittäminen Tärkeimmät tehtävät ➢ Tietoturvallisuuden hallinnan kattavuuden ja rajojen alustava määrittäminen. Tärkeimmät lopputulokset ➢ Alustava kuvaus tietoturvallisuuden hallinnan kattavuudesta. Kuvausta täydennetään tarvittaessa vaiheessa B1.
A3 Tietoturvallisuuden hallinnan roolien ja vastuiden alustava määritys Tärkeimmät tehtävät ➢ Määritetään alustavasti tietoturvallisuuden kannalta tärkeimmät toiminnot ja niiden vastuuhenkilöt. Varmistetaan organisoinnin riittävä kattavuus (ks. A2). Tehtävän voi yhdistää vaiheeseen D1. Tärkeimmät lopputulokset ➢ Alustava luettelo tärkeimmistä tietoturvallisuuteen liittyvistä rooleista, vastuista ja valtuuksista.
A4 Projektisuunnitelman laatiminen Tärkeimmät tehtävät ➢ Projektisuunnitelman laatiminen ➢ Projektiorganisaation muodostaminen. Tärkeimmät lopputulokset ➢ Projektisuunnitelma ➢ Projektiorganisaatio
A5 Johdon hyväksynnän hankkiminen projektin aloittamiselle Tärkeimmät tehtävät ➢ Johdon hyväksynnän ja tuen hankkiminen tietoturvallisuuden kehittämisprojektille ➢ Projektisuunnitelman hyväksyminen. Tärkeimmät lopputulokset ➢ Pöytäkirja tmv. projektisuunnitelman hyväksymisestä.
B Tärkeiden toimintojen, riippuvuuksien ja tieto-omaisuuden tunnistaminen
B1 Tietoturvallisuuden hallinnan kattavuuden ja riippuvuuksien määrittäminen Tärkeimmät tehtävät ➢ Tärkeimpien sidosryhmien ja riippuvuuksien kuvaaminen. ➢ Vaiheessa A2 aloitetun työn tietoturvallisuuden hallinnan kattavuusmäärittelyn viimeistely. Tärkeimmät lopputulokset ➢ Kuvaus tärkeimmistä tietoturvallisuuden sidosryhmistä ja riippuvuussuhteista. ➢ Kuvaus tietoturvallisuuden hallinnan kattavuudesta.
B2 Tärkeiden toimintojen, tieto-omaisuuden ja turvakontrollien kuvaaminen Tärkeimmät tehtävät ➢ Tärkeiden toimintojen ja tieto-omaisuuden kartoittaminen. ➢ Olemassa olevien/vaadittavien turvakontrollien kuvaaminen.

Tärkeimmät lopputulokset ➢ Kuvaus organisaation tärkeimmistä toiminnoista, suojattavista kohteista ja näihin liittyvistä turvakontrolleista.
B3 Teknisen ja fyysisen tietojenkäsittely-ympäristön kuvaaminen. Tärkeimmät tehtävät ➢ Tärkeitä toimintoja tukevan teknisen ja fyysisen tietojenkäsittely-ympäristön kuvaaminen. ➢ Tärkeiden resurssien teknisten turvakontrollien kuvaaminen. Tärkeimmät lopputulokset ➢ Kuvaus tai kooste teknisestä ja fyysisestä tietojenkäsittely-ympäristöstä turvajärjestelyineen.
B4 Tietoturvallisuuden nykytilanteen ja vaatimustenmukaisuuden arviointi Tärkeimmät tehtävät ➢ Tietoturvallisuuden nykytilanteen sekä vaatimustenmukaisuuden arviointi ja raportointi johdolle Tärkeimmät lopputulokset ➢ Arvio siitä miltä osin tietoturvallisuutta tulee organisaation tarpeisiin, toimintoihin ja suojattaviin kohteisiin nähden parantaa.
B5 Tietoturvapolitiikan päivitys tai laatiminen Tärkeimmät tehtävät ➢ Tietoturvapolitiikan tarkistaminen ja tarvittaessa päivittäminen. ➢ Tietoturvaperiaatteiden päivittäminen ja täydentäminen. Tärkeimmät lopputulokset ➢ Johdon hyväksymä tietoturvapolitiikka (voidaan tehdä aikaisemmin tai myöhemmin). ➢ Ajantasaiset ja riittävän kattavat tietoturvaperiaatteet.
C Riskienhallinta- ja häiriötilannemenettelyjen luominen
C1 Riskienhallinta- ja häiriötilannehallintamenettelyjen määrittäminen sekä kuvaaminen Tärkeimmät tehtävät ➢ Riskienhallinta- ja häiriötilannemenettelyjen määrittäminen, suunnittelu sekä kuvaaminen. Tärkeimmät lopputulokset ➢ Kuvaus riskienhallinta- ja häiriötilannemenettelyistä. Kriteerit riskien hyväksymiseksi. Menetelmät poikkeamien havaitsemiseksi ja hallitsemiseksi. ➢ Henkilöstön ohjeistus riskien havaitsemiseksi ja ilmoittamiseksi.
C2 Riskien tunnistaminen ja analysointi Tärkeimmät tehtävät ➢ Riskien arviointi Tärkeimmät lopputulokset ➢ Riskianalyysi
C3 Riskienhallinta-toimenpiteiden suunnittelu ja turvakontrollien valinta Tärkeimmät tehtävät ➢ Riskienhallinnan suunnittelu ja turvakontrollien valinta. ➢ Jäännösriskien arviointi. Tärkeimmät lopputulokset ➢ Riskienhallintasuunnitelma ja kuvaus valituista turvakontrolleista.
C4 Jäännösriskien ja tärkeimpien turvakontrollien hyväksyttäminen johdolla Tärkeimmät tehtävät ➢ Hyväksyttävän riskitason päättäminen. ➢ Tietoturvallisuuden jäännösriskien hyväksyttäminen johdolla. Tärkeimmät lopputulokset ➢ Dokumentti hyväksymisestä, esim. hyväksymispöytäkirja.
C5 Tietoturvallisuuden viitekehyksen valinta, soveltamissuunnitelman laatiminen Tärkeimmät tehtävät ➢ Soveltamissuunnitelman laatiminen valitun viitekehyksen mukaan, työtä jatketaan vaiheiden D aikana. Tärkein lopputulos

➢ Soveltamissuunnitelma
D Tietoturvallisuuden hallintamenettelyjen luominen
D1 Tietoturvaorganisaation, roolien ja vastuiden sekä valtuuksien määritys Tärkeimmät tehtävät ➢ Vaiheessa A3 aloitettu tietoturvaorganisaation määrittäminen ja kuvaaminen loppuun. Jos tämä on jo tehty, päivitetään tarvittaessa. Tärkeimmät lopputulokset ➢ Kuvaus tietoturvallisuuden organisoinnista, rooleista, vastuista sekä valtuuksista. ➢ Tietoturvaorganisaatio.
D2 Resursoinnin tarkistaminen ja tietoturvallisuuden sisällyttäminen taloussuunnitteluun Tärkeimmät tehtävät ➢ Tarkistetaan, onko vastuissa ja organisoinnissa riittävä kattavuus. ➢ Tietoturvallisuuden hallintaan ja ylläpitoon tarvittavien resurssien riittävyyden arviointi. Tärkeimmät lopputulokset ➢ Yhteenveto tietoturvallisuuden hallintaan ja ylläpitoon tarvittavien resurssien riittävyydestä.
D3 Auditoinnin, katselmointien ja mittaamisen suunnittelu Tärkeimmät tehtävät ➢ Auditoinnin, katselmointien, valvonnan ja mittaamisen suunnittelu sekä kuvaaminen. Tärkeimmät lopputulokset ➢ Auditointi-, katselmointi- ja mittaamisperiaatteet ja suunnitelmat.
D4 Yhteistyön, hankintatoiminnan ja raportointimenettelyjen suunnittelu Tärkeimmät tehtävät ➢ Yhteistyön, hankintatoiminnan ja raportointimenettelyjen suunnittelu. Tärkeimmät lopputulokset ➢ Tietoturva-asioita käsittelevä yhteistyöryhmä (ellei ole jo aikaisemmin perustettu). ➢ Tietoturvallisuuden yhteistyöryhmän ja johdon tietoturvallisuuteen liittyvät kokouskäytännöt. ➢ Ohjeistus tietoturvallisuuden huomioimisesta kumppanuus- ja hankintatoiminnassa. ➢ Kuvaus raportointimenettelystä ja mallipohja sidosryhmäraporttia varten.
D5 Tietoturvallisuuden hallinnan dokumentoinnin sekä tiedottamisen suunnittelu Tärkeimmät tehtävät ➢ Tietoturvallisuuden hallinnan dokumentoinnin ja tiedottamisen suunnittelu. Tärkeimmät lopputulokset ➢ Suunnitelma tai kuvaus tietoturvallisuuden hallinnan dokumentoinnista ja tiedottamisesta.
D6 Henkilöstön koulutuksen, ohjauksen ja tuen suunnittelu Tärkeimmät tehtävät ➢ Henkilöstön koulutuksen suunnittelu, henkilöstöturvallisuuden varmistaminen, riittävän ohjeistuksen varmistaminen. Tärkeimmät lopputulokset ➢ Työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti. ➢ Henkilöstön koulutussuunnitelma. ➢ Koulutusrekisteri ➢ Suunnitelmat ja ohjeistot henkilöstöturvallisuuden ylläpitoon sekä parantamiseen.
D7 Tietoturvaperiaatteiden päivittäminen, hyväksyttäminen ja julkaisu Tärkeimmät tehtävät ➢ Tietoturvapolitiikan viimeistely, hyväksyttäminen ja julkaisu. (Ellei ole jo aikaisemmin tehty). ➢ Tietoturvaperiaatteiden tarkistaminen ja tarvittaessa täydentäminen. Tärkeimmät lopputulokset ➢ Hyväksytty ja julkaistu tietoturvapolitiikka. Ajantasaiset tietoturvaperiaatteet.
D8 Tietoturvallisuuden ylläpito- ja kehittämissuunnitelman laatiminen Tärkeimmät tehtävät ➢ Tietoturvallisuuden ylläpito- ja kehittämissuunnitelman laatiminen sekä

hyväksyminen. Tärkeimmät lopputulokset ➢ Tietoturvallisuuden ylläpito- ja kehittämissuunnitelma. ➢ Viimeistellään vaiheessa C5 aloitettu soveltamissuunnitelma.

Taulukko 9 Projektimallin osa-alueet ja tehtävät.

A Tietoturvatarpeiden ja lähtökohtien tunnistaminen

Yleistä osa-alueesta A

Tietoturvallisuuden hallinnan kehittäminen edellyttää organisaatiolta muutoksia ja panostusta linjaorganisaatiosta. Tehtävä työ ja erityisesti sen arvo tulee voida perustella johdolle ja tarvittaessa muulle organisaatiolle. Ensimmäisessä vaiheessa kootaan ne lähtötiedot ja tekijät jotka ohjaavat tietoturvallisuuden kehittämistyötä.

A1 Tietoturvallisuuden lähtökohtien määrittäminen ja kuvaaminen

Tehtävät

- Tunnistetaan sisäiset ja ulkoiset toimintaan kohdistuvat tietoturvallisuuden erityis-vaatimukset.
- Esitellään tärkeimmät tietoturvavaatimukset organisaation johdolle.
- Määritellään organisaation tietoturvatavoitteet.
- Suunnitellaan, miten vaatimukset ja tavoitteet kohdistetaan organisaatiossa.
- Valitaan tai suunnitellaan tietoturvaluokittelu.

Vaiheen lopputulokset

- Lyhyt yhteenveto tietoturvallisuuden kannalta merkittävistä vaatimuksista.
- Kuvaus organisaation tietoturvatavoitteista (hyväksytetään johdolla).
- Suunnitelma tietoturvavaatimusten ja tavoitteiden kohdistamisesta (hyväksytetään johdolla).
- Kuvaus tietoturvaluokittelusta (hyväksytetään johdolla).

Sisäiset ja ulkoiset toimintaan kohdistuvat erityisvaatimukset

Merkittävimmät erityisvaatimukset voivat löytyä esim.

- lainsäädännöstä (ks. Finlex –säädöstietopankki),
- organisaation ja yksiköiden työjärjestyksistä,
- viranomaismääräyksistä,
- kriteeristöistä (joita toiminnassa noudatetaan),
- sopimuksista,
- sitoumuksista,
- organisaation omista linjauksista ja strategioista (mm. liiketoiminta ja tekniikka),
- organisaation johtamisjärjestelmistä,
- alihankinta- ja yhteistyöverkostojen tietoturvavaatimuksista,
- tunnistetuista riskeistä.

Tietoturvallisuuteen liittyvän lainsäädännön sekä viranomaisvaatimusten seuranta tulee vastuuttaa. Tarvittaessa seurantavastuu voidaan kirjata henkilön tehtäväkuvaukseen.

Tärkeimpien tietoturvavaatimusten esittely

Johdon tulee olla tietoinen toimintaan kohdistuvista erityisvaatimuksista. Vaatimukset voidaan kuvata esim. lyhyeksi yhteenvedoksi. Yhteenveto tulisi esitellä johdolle viimeistään siinä vaiheessa, kun tietoturvallisuuden kehitysprojektia perustellaan.

Organisaation tietoturvatavoitteiden määrittäminen
Johto määrittää tietoturvallisuuden ydintavoitteet. Ne ohjaavat organisaation eri tasojen ja toimintojen tietoturvatavoitteita. Toiminnoista vastaavien tehtävänä on huolehtia siitä, että he ottavat tietoturvavaatimukset ja tavoitteet huomioon vastuualueellaan.

Tietoturvatavoitteita voi pohtia mm. seuraavilla kysymyksillä:

- Mitkä ovat toimintaan kohdistuvat tietoturvavaatimukset?
- Millä tavoin tietoturvallisuus parantaa organisaation ydintavoitteiden saavuttamista?
- Miten tietoturvallisuuden hallinnalla vaikutetaan organisaation toiminnan laatuun (ja kilpailutekijöihin)?
- Onko organisaatiossa joitakin toimintoja tai muita kohteita, joita voidaan suojata tietoturvallisuuden hallinnan avulla?
- Onko tiedossa joitakin ei-toivottuja tapahtumia, joita voidaan hallita tietoturvallisuuden hallinnan avulla?
- Onko tiettyjä velvoitteita tai sitoumuksia, joihin vaikutetaan tietoturvallisuuden hallinnan avulla?
- Onko organisaatiossa jatkuvuuden varmistamiseen liittyviä vaatimuksia?
- Onko nykyisessä tietoturvallisuuden hallinnassa jotakin sellaista, jota tulisi erityisesti parantaa?

Vaatimusten ja tavoitteiden kohdistaminen organisaatiossa

Vaatimusten ja tavoitteiden kohdistaminen kannattaa suunnitella ainakin seuraaviin osa-alueisiin:

- toimintaan (prosessit, tarjottavat palvelut jne.),
- organisointiin ja vastuisiin,
- ohjeisiin,
- riskienhallintaan,
- dokumentointiin,
- turvallisuuspolitiikkaan,
- yhteistyöhön ja sopimuksiin,
- henkilöstölle tiedottamiseen ja kouluttamiseen.

Vaatimukset ja tavoitteet voidaan kohdistaa esim. kuvaamalla ne

- tietoturvallisuuden ylläpito- ja kehittämissuunnitelmassa,
- muissa suunnitelmissa,
- linjauksissa,
- tuloskorteissa,
- tehtäväkuvauksissa,
- menettelyohjeissa,
- sopimuksissa ja
- hankinta-asiakirjoissa.

Tietoturvatavoitteille tulee suunnitella aikataulu ja vastuut. Määrittämällä mittarit ja seurantatapa varmistetaan, että tavoitteiden toteutumista voidaan arvioida. Toteutumisen seuranta suunnitellaan viimeistään vaiheessa D3 (Auditoinnin, katselmointien ja mittaamisen suunnittelu). Tärkeimmät vaatimukset tulee ottaa huomioon henkilöstön koulutuksessa sekä tiedottamisessa.

Asetus tietoturvallisuudesta valtionhallinnossa edellyttää asetuksessa kuvattujen suojaustasoluokitusten käyttöä, mikäli organisaatio päättää luokitella asiakirjat. Tietoturvallisuusasetuksen lisäksi valtionhallinnossa sovelletaan mm. VAHTI 2/2010 liitteen 5

turvallisuusluokitusta sekä KATAKRIa (kansallinen turvallisuusauditointikriteeristö). Organisaatiossa voidaan käyttää myös muita luokituksia. Luokituksen suunnittelussa on suositeltava huomioida niiden yhteensopivuus tehtäessä yhteistyötä muiden organisaatioiden kanssa.

A2 Tietoturvallisuuden hallinnan kattavuuden määrittäminen

Tehtävä
Tietoturvallisuuden hallinnan kattavuuden ja rajojen alustava määrittäminen.

Vaiheen lopputulos
Kuvaus tietoturvallisuuden hallinnan kattavuudesta.

Kuvausta täydennetään tarvittaessa vaiheessa B1 ”Tietoturvallisuuden hallinnan kattavuuden ja riippuvuuksien määrittäminen”.

Tietoturvallisuuden hallinnan kattavuuden määrittäminen

Tietoturvallisuuden hallinnan kattavuus ja rajaukset määrittää, millaista kokonaisuutta tietoturvallisuuden hallinta koskee. Kattavuus voidaan kuvata esim. organisaation, sen sijainnin tai toimintojen mukaan. Tietoturvallisuuden hallintaa ei tule pilkkoa sellaisiin kokonaisuuksiin, joissa oleellisia organisaation osia tai vastuita jää pois.

Tietoturvallisuuden hallintakokonaisuutta suunniteltaessa voidaan pohtia seuraavia asioita:

- Millaiset valtuudet organisaation johto antaa tietoturvallisuuden hallinnan kattavuudelle (kattaako esim. koko toiminnan, vai sen osan)?
- Kohdistuuko organisaatioon ulkoisia vaatimuksia, jotka vaikuttavat tietoturvallisuuden hallinnan kattavuuteen?
- Onko olemassa muita johtamisjärjestelmiä, jotka tulisi ottaa huomioon (esim. riskienhallinta tai laadunhallinta)?
- Onko tietoturvallisuuden hallinnasta vastaavilla henkilöillä rooleja muissa organisaation toiminnoissa/yksiköissä?
- Onko joitakin kriittisiä toimintoja, jotka tulee erityisesti ottaa huomioon?

A3 Tietoturvallisuuden hallinnan roolien ja vastuiden alustava määrittäminen

Tehtävä
Määritellään alustavasti tietoturvallisuuden kannalta tärkeimmät toiminnot ja niiden vastuuhenkilöt. Varmistetaan organisoinnin riittävä kattavuus (ks. A2).

Tehtävän voi yhdistää vaiheeseen D1 (Tietoturvaorganisaation, roolien, vastuiden ja valtuuksien määritys).

Vaiheen lopputulos
Alustava luettelo tärkeimmistä tietoturvallisuuteen liittyvistä rooleista, vastuista valtuuksista (johto hyväksyy).

Tietoturvallisuuden hallinnan roolit

Vastuuhenkilöillä tulee olla tehtäväänsä riittävät valtuudet ja toimiva raportointisuhde ylimpään johtoon. Sen vuoksi rooleihin tulisi hankkia ylemmän johdon hyväksyminen. On tärkeää, että vastuuhenkilöillä on tehtäviinsä riittävä osaaminen. Sen vuoksi voidaan jo alkuvai-

heessa pohtia, onko vastuuhenkilöitä tarpeen kouluttaa lisää tehtäviinsä. Koulutusasioita on käsitelty tarkemmin tehtävässä D6.

Tässä vaiheessa voidaan määrittää vastuuhenkilöt niihin tehtäviin, jotka on tähän mennessä valittu toteutettaviksi. Sen lisäksi tulisi suunnitella vastuuhenkilöt seuraaviin tehtäviin:

- tietoturvallisuuden kehittäminen,
- tietoturvavaatimusten seuranta ja arviointi,
- tietoturvallisuudesta raportointi,
- tietoturvapoikkeamien käsittely,
- tietoturvayhteistyö (sisäinen ryhmä),
- jatkuvuussuunnitelmien laatiminen, päivitys ja katselmointi,
- laitteiden, rekistereiden ja tietojärjestelmien omistajuus,
- laite-, tietojärjestelmä-, palvelu-, ja ohjelmistoluetteloiden ylläpito,
- lain mukaisten selosteiden ja kuvausten päivitys,
- tietoturvallisuuteen liittyvien ohjeiden ylläpito,
- laitteiden ja tietojärjestelmien päivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus,
- laitteiden ja tietojärjestelmien muutostarpeiden seuranta, muutospäätösten teko ja muutosten toteutus,
- ICT-järjestelmien häiriöiden selvitys ja niistä toipuminen,
- kumppanuus- ja hankintatoiminta.

Vastuiden määrittämisessä tulee huomioida varahenkilöjärjestelyt. Vastuuhenkilöistä tulee pitää ajantasaista luetteloa ja organisaatiossa tulee olla menettelytapa henkilöstömuutoksista ilmoittamiseen.

Projektin rooleja ja vastuita on käsitelty kohdassa A4.

A4 Projektisuunnitelman laatiminen ja projektiorganisaation muodostaminen

Tehtävät
- Projektisuunnitelman laatiminen tietoturvallisuuden hallinnan kehittämiseen.
- Projektiorganisaation muodostaminen.

Vaiheen lopputulokset
- Projektisuunnitelma (johto hyväksyy).
- Projektiorganisaatio.

Projektin organisointi

Alkuvaiheessa on tärkeää kuvata projektin kannalta merkittävimmät avainhenkilöt sekä varmistaa, että he ovat tietoisia roolistaan. Tietoturvallisuuden hallintaprojektin alussa työtä voidaan tehdä pienelläkin projektiryhmällä, mutta projektin edetessä työ vaatii osallistumista myös linjaorganisaatiolta. Organisoinnin suunnittelussa voidaan tehdä seuraavia kysymyksiä:

- Miten projektin ohjaus ja raportointi toteutetaan?
- Onko suunnitellulla projektiryhmällä riittävät valtuudet toimia organisaatiossa?
- Onko ryhmän jäsenillä riittävästi aikaa ja motivaatiota tehtävään?
- Onko ryhmässä riittävää osaamista tehtäviin?
- Onko tehtäviä, joihin halutaan käyttää ulkopuolista asiantuntijaa?
- Onko organisaation ulkopuolella sidosryhmiä, jotka voivat auttaa projektissa?
- Tarvitseeko projekti ”sponsorin”, henkilön jonka osallistuminen projektin ohjaukseen vaikuttaa positiivisesti muiden asenteeseen projektia kohtaan?

Projektisuunnitelma

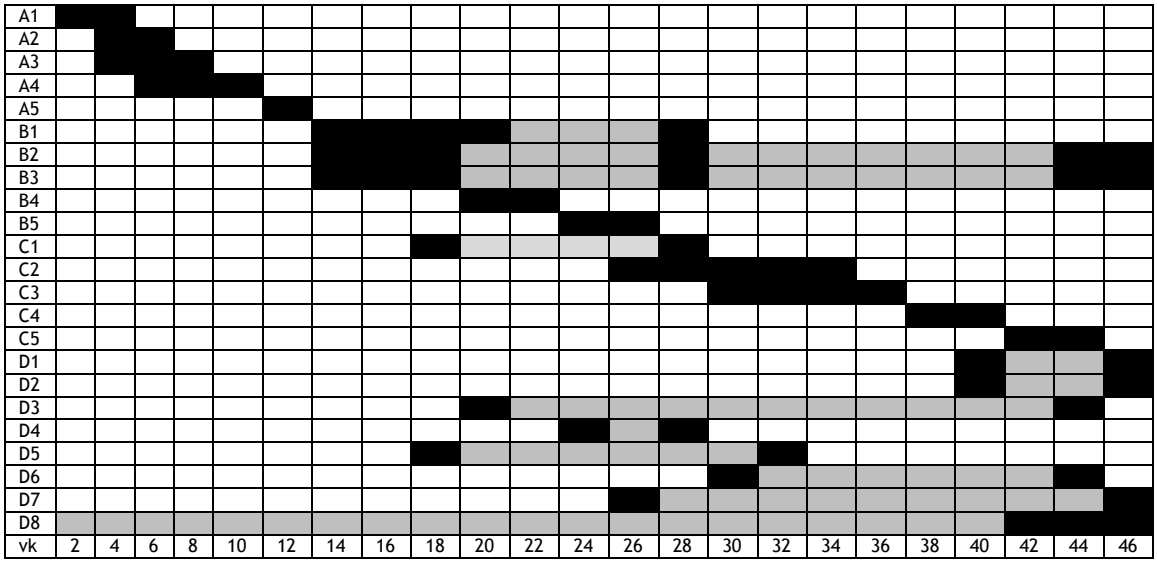
Projektisuunnitelmassa määritetään selkeät tavoitteet ja varmistetaan, että työn toteuttamiseen on riittävät resurssit. Työtä ohjaa organisaation johto joko linjaorganisaation kautta tai esim. ohjausryhmätyöskentelynä. Projektisuunnitelman tulee tukea organisaation omaa toimintaa. Vaikka projektin tavoitteena olisikin täyttää jonkin kriteeristön vaatimukset, suunnittelua ei kannata tehdä suoraan kriteeristön tai standardin pohjalta esim. numerojärjestyksessä. Mikäli projekti tähtää jonkun kriteeristön täyttämiseen, voidaan sen vaatimukset kuitenkin priorisoida, vastuuttaa ja aikatauluttaa esim. erilliseen soveltamissuunnitelmaan (ks. C5).

Projektisuunnitelman sisältö voi olla esim. seuraava:

- kuvaus nykytilasta, tietoturvavaatimuksista ja tarpeista,
- päämäärät ja tavoitteet,
- hyödyt organisaatiolle,
- alustava arvio projektin kattavuudesta,
- projektin tavoitteiden kannalta kriittiset tekijät,
- projektin yleiskuvaus,
- alustava toteuttamissuunnitelma,
- projektin roolit ja vastuut,
- tarvittavat resurssit,
- aikataulu ja vaiheistus välitavoitteineen,
- kustannusarvio,
- kriittiset menestystekijät.

Projektin vaiheistus

Alla on esitetty esimerkki vaiheistuksesta. Tummennettu ruutu tarkoittaa aktiivista vaihetta Aktiivisessa vaiheessa voi myös olla taukoja tai työ vähemmän intensiivistä (harmaa alue). Alas on kuvattu viikot parillisina numeroina. Huom. ajankohta ja tehtävien kesto ovat viitteellisiä.



Kuvio 10 Esimerkki vaiheistamisesta. Vaiheistamisen suunnitteluun voi myös käyttää soveltamissuunnitelmaa. Siitä on esimerkki tehtäväosassa C5.

A5 Johdon hyväksynnän hankkiminen projektin aloittamiselle

Tehtävät
- Johdon hyväksynnän ja tuen hankkiminen tietoturvallisuuden kehittämisprojektille
- Projektisuunnitelman hyväksyminen

Vaiheen lopputulos
Pöytäkirja tmv. projektisuunnitelman hyväksymisestä

Johdon hyväksynnän ja tuen hankkiminen

Mitä enemmän tietoturvallisuuden kehittäminen tukee organisaation ydintavoitteita, sitä helpommin se saa organisaation johdon hyväksynnän. Tietoturvallisuudesta viestimiseen kannattaa kiinnittää erityistä huomiota. Näin varmistetaan, että vaikeatkin asiat ymmärretään oikein.

Oppaan aikaisemmissa vaiheissa on kuvattu niitä tietoja, joilla tietoturvallisuuden kehittämistarpeet perustellaan johdolle.

Projektia perustettaessa, voi varautua esimerkiksi seuraavanlaisiin kysymyksiin:
- Mistä projektissa on kyse?
- Mitä hyötyä projektista on organisaatiolle, entä sen asiakkaille?
- Vaikeuttaako tietoturvallisuuden kehittäminen henkilöstön toimintaa?
- Mitä kustannuksia projektista aiheutuu?
- Mitä seurauksia on sillä, jos tätä projektia ei toteuteta?
- Vaatiiko tämä merkittävää panosta henkilöstöltä, entä johdolta?

Projektista kannattaa tehdä lyhyt esittelymateriaali. Esitystä voi hyödyntää myöhemmin projektin aikana. Kun projekti on hyväksytty, siitä voi tiedottaa esim. organisaation intranetissä.

B Tärkeiden toimintojen, riippuvuuksien ja tieto-omaisuuden tunnistaminen

Yleistä osa-alueesta B

Vaiheen B tehtävänä on selvittää tietoturvallisuuden nykytilanne sekä kuvata ja analysoida organisaatiota kehittämistoimenpiteiden suunnittelua varten.

B1 Tietoturvallisuuden hallinnan riippuvuuksien määrittäminen

Tehtävä
- Tärkeimpien sidosryhmien ja riippuvuuksien kuvaaminen.
- Vaiheessa A2 aloitettu tietoturvallisuuden hallinnan kattavuuden määrittämisen viimeistely.

Vaiheen lopputulos
- Kuvaus tärkeimmistä sisäisistä ja ulkoisista tietoturvallisuuden sidosryhmistä ja riippuvuussuhteista.
- Kuvaus tietoturvallisuuden hallinnan kattavuudesta.

Merkittävät sidosryhmät

Mitä verkottuneempaa toiminta on ja mitä enemmän toiminta on riippuvaista organisaation ulkopuolisista toimijoista, sitä tärkeämpää on tuntea tärkeimmät sidosryhmät.

Sidosryhmien osalta tietoturvallisuuden hallinnan tulisi kattaa ainakin tärkeät sidosryhmäsuhteet, ulkoistetut palvelut ja tiedonvaihto sekä raportointisuhteet eri toimijoiden kesken.

Tietoturvallisuuden sisäisiä ja ulkoisia sidosryhmiä voivat olla esim. (ks. D4)

- johto,
- tietoturvallisuuden yhteistyöryhmä,
- henkilöstö,
- asiakkaat,
- yhteistyökumppanit,
- palvelutoimittajat, alihankkijat ja
- viranomaiset.

Tietoturvallisuuden hallinnan kattavuuden viimeistely

Vaiheessa A2 on kuvattu tietoturvallisuuden hallinnan kattavuus alustavasti. Kun merkittävät sidosryhmät on tunnistettu, voidaan vielä tarkistaa, että tietoturvallisuuden hallinta on riittävän kattavaa. Organisaatio voi myös tehdä päätöksen laajentaa tietoturvallisuuden hallinnan kattavuutta myöhemmässä vaiheessa.

B2 Tärkeiden toimintojen, tieto-omaisuuden ja turvakontrollien kuvaaminen

Tehtävät

- Tärkeiden toimintojen ja tieto-omaisuuden kartoittaminen.
- Olemassa olevien tai vaadittavien turvajärjestelyiden (turvakontrollien) kuvaaminen.

Vaiheen lopputulos
Kuvaus organisaation tärkeimmistä toiminnoista, suojattavista kohteista ja näihin liittyvistä turvakontrolleista.

Tietojen kokoaminen

Organisaation tärkeimmät toiminnot (ydintoiminnot, ydinprosessit) on usein kuvattu työjärjestyksessä. Viimekädessä organisaation johto määrittää, mitkä ovat toiminnan kannalta tärkeimmät toiminnot. Toiminnoilla tulee olla vastuuhenkilöt. Heiltä ja toimintojen muilta asiantuntijoilta kysymällä voidaan selvittää tärkeimmät tiedot.

Tulosten ja kuvausten dokumentointi kannattaa suunnitella niin, että ne ovat myöhemmin helposti ylläpidettäviä. Mitä lähemmin ne liittyvät organisaation päivittäiseen toimintaan, sitä luontevammin niitä päivitetään. Kuvauksia on suositeltavaa katselmoida ja tarvittaessa päivittää vähintään kerran vuodessa.

Seuraavalla sivulla on esitetty yksinkertainen tiedonkeruukortti. Sen avulla voidaan koota tärkeimmät tiedot toiminnoista ja kriittisestä tieto-omaisuudesta. Mikäli tietojen kokoamisen yhteydessä havaitaan merkittäviä riskejä, on suositeltava tarkistaa riskit erikseen. Riskien kirjaamisesta ja seurannasta on esimerkki tehtävässä C3.

Tietokortti	
Yksikön/toiminnon nimi	Vastuuhenkilö(t)
Kuvaa lyhyesti toiminta/vastuualueet	
Mitkä ovat toimintaan kohdistuvat erityisvaatimukset (säädökset, sopimukset, tietoturvavaatimukset)?	
Mitkä ovat toiminnan kannalta välttämättömiä, mitä ilman toimintaa ei pystytä tekemään (perustele)? Miten välttämättömät asiat on suojattu?	
Jos toiminnassa on häiriöitä, mihin/keihin se ensisijaisesti vaikuttaa?	
Mitä vaikutuksia on tietojen joutumisella ulkopuolisten tai asiattomien käsiin? Mistä tiedoista tällöin on kyse?	
Arvioi vakavuus 1-5 (1=ei erityistä merkitystä, 5=erittäin kriittinen)	
Arvioi todennäköisyys 1-5 (1=ei todennäköinen, 5=erittäin todennäköinen)	
Onko joitakin asioita, jotka erityisesti altistavat tällaiselle vahingolle? Jos on, niin kerro, mitkä:	
Miten tähän on varauduttu?	
Mitä vaikutuksia on 1) tietojen puutteellisuudella tai 2) sillä, että niiden todenperäisyydestä ei ole varmuutta tai 3) ne ovat muuttuneet virheellisiksi? Kerro, millaisista tiedoista olisi kyse.	
Arvioi vakavuus 1-5 (1=ei erityistä merkitystä, 5=erittäin kriittinen)	
Arvioi todennäköisyys 1-5 (1=ei todennäköinen, 5=erittäin todennäköinen)	
Onko joitakin asioita, jotka erityisesti altistavat tällaiselle vahingolle? Jos on, niin kerro, mitkä:	
Miten tähän on varauduttu?	
Mitkä järjestelmät tai palvelut ovat kriittisiä, jos ne ovat pois päältä tai eivät ole käytettävissä? Kerro vaikutuksista.	
Alle 2 tuntia	
Päivä	
Viikko	
Miten tähän on varauduttu?	
Tietoturvapäällikkö täyttää: Tietoturvallisuuden ylläpito- ja kehittämissuunnitelmassa huomioitavat erityisvaatimukset ja tavoitteet; Suojattavien kohteiden turvallisuusluokittelu ja pääasiallinen tietoaineistojen suojaustasoluokka (mikäli tietoja luokitellaan).	

Tietokortti tärkeän tieto-omaisuuden kartoittamiseksi.

B3 Teknisen ja fyysisen tietojenkäsittely-ympäristön kuvaaminen

Tehtävät

- Tärkeitä toimintoja tukevan teknisen ja fyysisen tietojenkäsittely-ympäristön kuvaaminen.
- Tärkeiden resurssien teknisten turvakontrollien kuvaaminen.

Vaiheen lopputulos
Kuvaus tai kooste teknisestä ja fyysisestä tietojenkäsittely-ympäristöstä turvajärjestelyineen
.

Teknisen ja fyysisen ympäristön dokumentointi

Teknisen ja fyysisen ympäristön kuvauksissa tulisi välttää päällekkäistä dokumentointia, koska se hankaloittaa tiedon ylläpitämistä. Tietoturvallisuuden kehittämisestä vastaava voi ylläpitää esim. tietoturvakäsikirjassa tietoa, mistä tietoturvallisuuden kannalta tärkeimmät tiedot löytyvät.

Tietojenkäsittely-ympäristön tekniseen ja fyysiseen dokumentointiin voivat kuulua esim.

- järjestelmäkuvaukset,
- arkkitehtuurikuvaukset,
- tietoliikenteen topologiakuvaukset,
- tietoturvapäivityksien ja haavoittuvuuksien hallinnan periaatteet ja ohjeet,
- oletussalasanojen periaatteet ja ohjeet,
- rekisteriasetukset,
- versionhallinta,
- turva-asetukset ja turvallinen konfigurointi,
- järjestelmän asennusohjeistus,
- loki- ja arkistotietojen käsittelytavat,
- järjestelmän palautus- ja käynnistysmenettelyt,
- valtuuksien hakumenettelyt,
- operointiohjeet,
- tietoturvallisuuden valvontaan liittyvä dokumentaatio,
- kuvaus varmistuksista,
- jatkuvuus- ja toipumissuunnitelmat,
- palvelutoimittajien turvallisuuskuvaukset,
- fyysisten tilojen kuvaukset (sis. turvajärjestelyt),
- laitteiden fyysinen sijaintitieto.

B4 Tietoturvallisuuden nykytilanteen ja vaatimustenmukaisuuden arviointi

Tehtävä
Tietoturvallisuuden nykytilanteen sekä vaatimustenmukaisuuden arviointi ja raportointi johdolle.

Vaiheen lopputulos
Arvio siitä miltä osin tietoturvallisuutta tulee organisaation tarpeisiin, toimintoihin ja suojattaviin kohteisiin nähden parantaa.

Yhteenvetoa käytetään tietoturvallisuuden ylläpito- ja kehittämissuunnitelman laatimisessa.

Tietoturvavaatimusten arviointi

Tietoturvavaatimusten arvioinnissa selvitetään, toimiiko organisaatio sille asetettujen tai sen itse asettamien turvallisuusvaatimusten mukaisesti. Mahdollisista puutteista raportoidaan organisaation johdolle.

Arvioinnissa voidaan selvittää, miten organisaation toiminta vastaa niitä vaatimuksia, jotka tulevat

- lainsäädännöstä (ks. Finlex – säädöstietopankki),
- organisaation ja yksiköiden työjärjestyksistä,
- viranomaismääräyksistä,
- sopimuksista, sitoumuksista,
- organisaation omista linjauksista ja strategioista,
- organisaation luokituskäytännöistä ja suojaustasovaatimuksista,
- organisaation johtamisjärjestelmistä,
- alihankinta- ja yhteistyöverkostojen tietoturvavaatimuksista ja
- tunnistetuista riskeistä.

Alla olevassa taulukossa on yksinkertainen malli vaatimusten ja toiminnan arvioimiseen. Toimenpiteet kuvataan tarvittaessa tietoturvallisuuden ylläpito- ja kehittämissuunnitelmassa.

Vaatimus	Toteutuminen organisaatiossa	Vastuu	Toimenpiteet

Taulukko 10 Yksinkertainen malli vaatimusten ja toiminnan arviointitaulukosta.

B5 Tietoturvaperiaatteiden kuvaaminen

Tehtävä

- Tietoturvapolitiikan tarkistaminen ja tarvittaessa päivittäminen.
- Tietoturvaperiaatteiden päivittäminen ja täydentäminen.

Vaiheen lopputulos

- Johdon hyväksymä tietoturvapolitiikka
- Ajantasaiset ja riittävän kattavat tietoturvaperiaatteet

Tietoturvapolitiikka voi olla hierarkkinen kokonaisuus, joka koostuu useasta tasosta. Tietoturvapolitiikka –dokumentin ei tarvitse olla “Tietoturvapolitiikka” –niminen, vaikka nimitys on yleisesti käytössä. Politiikkadokumentti voi olla esim. yhden sivun mittainen johdon “julkilausuma”, jota täydennetään muilla periaatteilla. Se voi myös olla osa muita organisaation periaatteita, kuten riskienhallintapolitiikkaa.

Tietoturvapolitiikassa erityisesti kannattaa huomioida

- organisaation strategiat ja toiminnan tavoitteet,
- eri muodoissa olevat tiedot ja tiedon elinkaari,
- tietoturvallisuuden hallinnan kattavuus,
- tietoturvallisuuden liittyvät vaatimukset ja tavoitteet,
- organisaation rakenne ja toiminta,
- riskienhallintaperiaatteet,
- ohjaavuus jatkuvaan parantamiseen,
- johdon hyväksyminen.

Tietoturvapolitiikan tueksi voidaan määrittää periaatteita ja ohjeita. Alla on luettelo periaatteista, joita organisaatiossa on suositeltava harkita

- pääsynvalvonnan periaatteet,
- puhtaan pöydän ja näytön politiikka,
- ohjelmistojen asentamiseen ja lisensseihin liittyvät periaatteet,
- ohjelmistojen poistamista koskevat toimintaperiaatteet,
- varmuuskopiointia koskevat periaatteet,
- viestintäperiaatteet,
- hyväksyttävän käytön periaatteet,
- tietojen käsittelyperiaatteet,
- sähköpostipolitiikka,
- tietosuojapolitiikka,
- riskienhallintapolitiikka,
- sähköposti- ja internetin käytön periaatteet,
- kannettavia laitteita ja tallennusmedioita koskevat periaatteet,
- etäkäyttö- ja etätyöperiaatteet,
- salausmenetelmien käytön ja sallittujen menetelmien periaatteet,
- vaatimustenmukaisuutta koskevat periaatteet,
- toiminta väärinkäytöstilanteissa,
- teknisen valvonnan periaatteet.

C Riskienhallinta- ja häiriötilannemenettelyjen luominen

Yleistä osa-alueesta C

Vaiheessa C määritellään ja suunnitellaan, miten turvataan organisaatiolle tietoturvallisuuden kannalta tärkeät kohteet. Suunnittelu perustuu riskien arviointiin ja niiden hallintaan. Viimeistään tässä vaiheessa päätetään myös työvälineet, joiden avulla riskejä arvioidaan sekä seurataan.

Mikäli organisaatiossa on käytössä riskienhallintamenettelyt (ja mahdollisesti riskienhallintapolitiikka), kannattaa niitä hyödyntää mahdollisuuksien mukaan.

C1 Riskienhallinta- ja häiriötilannemenettelyjen määrittäminen sekä kuvaaminen

Tehtävä
Riskienhallinta- ja häiriötilannemenettelyjen määrittäminen, suunnittelu sekä kuvaaminen.

Vaiheen lopputulokset

- Kuvaus riskienhallinta- ja häiriötilannemenettelyistä. Kriteerit riskien hyväksymiseksi. Menetelmät turvallisuuspoikkeamien havaitsemiseksi ja hallitsemiseksi.
- Henkilöstön ohjeistus riskien havaitsemiseksi ja ilmoittamiseksi.

Riskienhallinta- ja häiriötilannemenettelyjen suunnittelu

Yksi riskienhallinnan tärkeimmistä tehtävistä on ongelmien ennaltaehkäisy ja riskien vaikutusten hallinta. On tärkeä muistaa, että riski ei aina ole negatiivinen ja poistettava, vaan sillä voi olla myös positiivisia vaikutuksia. Tärkeintä on hallita riskin negatiivisia vaikutuksia.

Riskienhallinta- ja häiriötilannemenettelyjä kuvatessa on suositeltava huomioida ainakin

- tunnetut haavoittuvuudet ja heikkoudet,
- eri turvallisuusolosuhteet (normaalitoiminta, erityistilanteet, onnettomuudet, hätätapaukset ja poikkeusolot)

- tunnetut, toistuvat ongelmat,
- sopimukset ja lakisääteiset vaatimukset ym. jotka tulee ottaa huomioon (ml. ICT-varautumisen vaatimukset),
- suojattavat kohteet,
- tunnetut uhkat,
- menetelmät turvallisuuspoikkeamien havaitsemiseksi sekä suojaavien ja korjaavien toimenpiteiden tekemiseksi.

ICT-varautumisen suunnittelu

Tietojenkäsittelyn häiriöihin voidaan varautua arvioimalla mahdollisia häiriötilanteita, suunnittelemalla ja toteuttamalla keinot häiriöistä selviämiseen sekä harjoittelemalla. Organisaation tulee tunnistaa kriittisimmät toiminnot ja niiden riippuvuudet tietotekniikasta.

Varautumisen suunnittelun tavoitteena on

- tunnistaa tekijöitä, jotka voivat aiheuttaa toiminnan keskeytyksiä tai muuten hankaloittaa toimintaa,
- suunnitella varajärjestelyt ,
- suunnitella keinot rajata vahinkoja ja palata mahdollisimman nopeasti normaalitoimintaan.

Toipumissuunnitelman tueksi voi käyttää esim. tehtävässä B2 esiteltyä tiedonkeruukorttia ja tehtävässä C3 esiteltyä riskikorttia.
Valmiussuunnittelun tavoitteena on mm.

- lakisääteisten valmiusvaatimusten täyttäminen,
- toiminnan jatkuvuuden varmistaminen poikkeusoloissa,
- suunnitella varajärjestelyt ja
- suunnitella keinot palautumiseen normaalitoimintaan.

Varautumissuunnitelmien päivitys ja katselmointi tulee olla vastuutettu ja organisoitu. Suunnitelmien toimivuutta tulee testata, harjoitella ja arvioida säännöllisesti.

Varautumissuunnitelmien toimivuutta on suositeltava tarvittaessa harjoitella yhteistyökumppaneiden kanssa. Harjoittelu voidaan kevyimmin toteuttaa esim. ”pöytäharjoituksena”, jossa esitetään kuviteltu tilanne ja osallistujia pyydetään kertomaan, miten he toimivat tilanteessa.

Menettelyt tietoturvapoikkeamiin

Tietoturvapoikkeamatilanteisiin tulee olla selkeät ohjeet. Ohjeissa tulee määrittää rooleittain, kuka selvittää tapahtunutta, kenen määräyksestä ja kuka päättää viranomaiskontakteista (esim. esitutkintapyynnön teosta) ja tiedottamisesta.

Tietoturvapoikkeamien käsittelyn organisointi lyhyesti:

- Muodosta tietoturvapoikkeamien käsittelyyn ryhmä.
- Kouluta ryhmän henkilöt.
- Harjoittele säännöllisesti.
- Sovi yhteistyö- ja raportointimenettelyt (sisäiset ja ulkoiset).
- Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa.
- Poikkeamista tehdään puolivuosittain yhteenveto johdolle (ks. tehtävä D4).
- Sovi seurannasta ja poikkeamien jälkikäteisanalyysistä.
- Varmista, että tapahtumista opitaan ja korjaavilla toimenpiteillä pyritään ehkäisemään vastaavaa tilannetta.
- Varmista, että jatkuvuussuunnitelmat ovat kunnossa.

C2 Riskien tunnistaminen ja analysointi

Tehtävä
Riskien arviointi.

Vaiheen lopputulos
Riskianalyysi

Riskien arviointi

Riskien arviointi tulisi olla säännöllistä. Ainakin ydintoimintoihin on suositeltava tehdä riskianalyysi vähintään kerran kolmessa vuodessa ja silloin, kun toiminta muuttuu merkittävästi. Riskienhallinnan periaatteet voidaan kuvata esim. riskienhallintapolitiikkaan.

Riskien arviointiin löytyy lukuisia välineitä. Tarkastelussa on suositeltava ottaa huomioon normaalitoiminnan lisäksi erityistilanteet, onnettomuudet ja hätätapaukset.

Riskien arviointia voidaan hyödyntää
- priorisointiin, organisaation turvallisuustoiminnan tavoitteiden asettamiseen,
- tietoturvaongelmien vaikutusten arviointiin ja turvatoimenpiteiden suunnitteluun,
- muutoshallintaan, hankintoihin, sopimuksiin, järjestelmäkehitykset ja koulutukseen.

Riskien raportointi

Riskien arvioinnin lisäksi henkilöstön omien havaintojen tekeminen ja valppaus on merkittävässä asemassa. Sen vuoksi riskien raportointi tulee organisoida niin, että tietoturvallisuudesta vastaava saa tiedon viivytyksettä. Merkittävät riskit voidaan kirjata esim. ”riskikorttiin” toimenpiteitä ja seurantaa varten. Riskikortista on esimerkki seuraavalla sivulla.

C3 Riskienhallinnan ja turvakontrollien suunnittelu

Tehtävä
Riskienhallinnan suunnittelu ja turvakontrollien valinta.

Vaiheen lopputulokset
- Riskienhallintasuunnitelma ja kuvaus valituista turvakontrolleista.
- Riskienhallintasuunnitelma voidaan sisällyttää tietoturvallisuuden ylläpito- ja kehittämissuunnitelmaan (ks. D8).

Riskienhallintasuunnitelma (tai tietoturvasuunnitelma) kuvaa ne tekniset ja hallinnolliset menettelyt, joilla hallitaan riskiä. Riskienhallintasuunnitelma voi olla erillinen dokumentti tai se voidaan sisällyttää tietoturvallisuuden ylläpito- ja kehittämissuunnitelmaan.

Riskienhallintasuunnitelman laatimiseen ja turvakontrollien valintaan tulisi varata riittävästi aikaa. Sellaisten turvakontrollien valintaan, jotka vaativat erityistä taloudellista panosta tai työmäärää, voidaan käyttää hyöty-kustannusanalyysiä. Merkittävien riskien kohdalla voidaan suunnitella erityinen riskienhallintatoimenpiteiden toteutuksen ja tehokkuuden valvonta.

Seuraavalla sivulla on esimerkki Excel – työkalusta, jolla kerätään riskitietoja ja tehdään päätöksiä. Oranssit osat täyttyvät automaattisesti ja ne opastavat kortin täyttäjää.

RISKIKORTTI *TÄMÄ OSA ON TARKOITETTU RISKIN KIRJAAJAN TÄYTETTÄVÄKSI*					
Kortin pvm.				*ID*	*1*
Laatija				*Tila*	*Kenttä täyttyy automaattisesti.*
Riskin nimi					
Riskin luonne	*Klikkaa tätä kenttää ja valitse riskin luonne nuolen alta esiin tulevasta alasvetovalikosta.*				
Riskin kuvaus					
Riskin seurausten vakavuus		*Selityskenttä*	*Todennäköisyys*		*Selityskenttä*
Riskin merkittävyys (vakavuus* todennäköisyys)	*0*		*Kenttä täyttyy automaattisesti.*		
Intressitahot					
Odotettavissa oleva menetys					
Riskin hallintakeinot					
Potentiaaliset muut hallintakeinot tai suositukset.					
Riskin omistaja/ vastuuhenkilö					
Viitteet					
Päätös	*Klikkaa ja valitse tästä*	*Kenttä täyttyy automaattisesti.*			
Päätöksen kuvaus/perustelu					
Päätöksen tekijä					
Päätöksen pvm.					

Yllä oleva taulukko on tarkoitettu riskitiedon keräämiseen, analysointiin ja riskienhallintatoimenpiteistä päättämiseen. Alla oleva taulukko on tarkoitettu riskin ja sen hallintatoimenpiteiden seurantaan. Työväline on veloituksetta saatavissa esim. Valtion IT-palvelukeskuksen tietoturvapalveluista.

RISKIN SEURANTATIEDOT *Riskienhallinnasta vastaava ylläpitää tätä osaa.*	
Riskipäätös	*Kenttä täyttyy automaattisesti.*
Kenttä täyttyy automaattisesti.	
Onko riskin tila hyväksyttävä?	*Klikkaa ja valitse.*
	Kenttä täyttyy automaattisesti.
Tehtävän tila	*Mikäli riskiä käsitellään tietyn tehtävän tai projektin sisällä, valitse tila tästä*
Tehtävän/projektin tunniste	
Vaatiiko erillisen kartoituksen?	*Klikkaa ja valitse.*

Lisätietoja riskin ja sen hallinnan tilasta	
Kenelle/minne raportoitu, kenen toimesta, miten ja milloin	
Kirjaa oikeanpuoleiseen ruutuun, mikäli riski on liitetty toiseen riskienhallintakokonaisuuteen tai siihen liittyy muita muutoksia, kuten esim. kortin poistaminen käytöstä.	

C4 Riskienhallintasuunnitelman ja tärkeimpien turvakontrollien hyväksyttäminen johdolla

Tehtävät
- Riskienhallintasuunnitelman ja tärkeimpien turvakontrollien hyväksyttäminen johdolla.
- Tietoturvallisuuden jäännösriskien hyväksyttäminen johdolla.

Vaiheen lopputulokset
- Dokumentti hyväksymisestä, esim. hyväksymispöytäkirja.
- Osa turvakontrolleista voidaan alkaa toteuttamaan tässä vaiheessa.

Riskinhallintasuunnitelma

Riskienhallintasuunnitelma hyväksytetään johdolla. Hyväksynnästä tulee jäädä merkintä. Turvatoimista huolimatta jää sellaisia riskejä, jotka organisaatio joutuu hyväksymään. Mikäli valinnalla on merkittäviä (liike)toimintavaatimuksia, tulee ne hyväksyttää johdolla. Johdon tulee lisäksi olla tietoinen päätöksen mahdollisista vaikutuksista.

Ne turvakontrollit, joilla on merkittäviä kustannusvaikutuksia tai jotka ovat muuten kriittisiä toiminnan kannalta, tulisi hyväksyttää organisaation johdolla.

C5 Viitekehyksen valinta, soveltamissuunnitelman laatiminen

Tehtävä
Soveltamissuunnitelman laatiminen valitun viitekehyksen mukaan.

Vaiheen lopputulos
Soveltamissuunnitelma

Tietoturvallisuuden viitekehystä ei ole välttämätöntä valita, mutta se helpottaa kokonaisuuden hallintaa ja auditointityötä. Mikäli organisaatio tavoittelee ISO/IEC 27001 –sertifikaattia, tulee soveltamissuunnitelma laatia sen mukaisesti. Kun tietoturvakokonaisuuden viitekehykseksi on valittu tunnettu kriteeristö tai muu lähde, on siihen nähden helpompi arvioida sekä kehittää omaa toimintaa. Viitekehyksenä voi toimia myös organisaation esim. riskienhallintakokonaisuus tai jokin liiketoimintaa ohjaava kokonaisuus.

Viitekehyksen kohta/vaatimus	Nykytila	Soveltaminen/ toimenpiteet	Ohjaavat dokumentit	Vastuu ja aikataulu	Toimenpiteen status

Esimerkki soveltamissuunnitelman rungosta.

D Tietoturvallisuuden hallintamenettelyjen luominen

Yleistä osa-alueesta D

Viimeisessä vaiheessa luodaan kokonaisuus, jolla tietoturvallisuutta hallitaan. Tämän vaiheen lopputuloksena syntyy tietoturvallisuuden kehittämissuunnitelma, jota seuraamalla tietoturvallisuuden parannustoimenpiteet otetaan vaiheittain käyttöön. Pitkän tähtäimen tietoturvallisuuden kehittämistä varten voidaan laatia tietoturvallisuuden kehitysohjelma (tietoturvastrategia) esim. viiden vuoden jaksolle.

D1 Tietoturvaorganisaation, roolien, vastuiden ja valtuuksien määritys

Tehtävä
Vaiheessa A3 aloitettu tietoturvaorganisaation määrittäminen ja kuvaaminen loppuun.

Mikäli tämä on jo tehty aikaisemmassa vaiheessa (A3), organisaatiota päivitetään tarvittaessa.

Vaiheen lopputulokset
- Kuvaus tietoturvallisuuden organisoinnista, rooleista, vastuista sekä valtuuksista.
- Tietoturvaorganisaatio.

Valtionhallinnossa organisaation tärkeimmät tehtävät on usein kuvattu työjärjestyksessä. Tietoturvallisuuteen liittyvät roolit ja vastuut on luontevinta liittyä henkilöiden normaaleihin työtehtäviin. Jokaisen työntekijän tulisi vastata oman vastuualueensa sekä tehtävien tietoturvallisuudesta, aivan kuten sen laadusta.

Vastuuhenkilöiden riittävästä koulutuksesta tulee varmistua. Vaikka tietoturvavastuut jakautuvat läpi organisaation, ylin vastuu tietoturvallisuudesta pysyy johdossa. Vastuu tietoturvallisuuden keskitetystä koordinoinnista voidaan keskittää yhdelle henkilölle (esim. tietoturvapäällikkö).

Tietoturva-asioita käsittelevä yhteistyöryhmä

Tietoturvapäällikön- tai vastaavan tärkeä sisäinen tuki on tietoturvaryhmä (voi olla eriniminen). Sen tehtävänä on kokoontua säännöllisesti (esim. neljä kertaa vuodessa). Tietoturvaryhmän tulisi tavata organisaation johto vähintään kaksi kertaa vuodessa.

Tietoturvaryhmän tehtävänä on
- edustaa organisaation eri tahojen tietoturvanäkemyksiä,
- sovittaa yhteen tietoturvavaatimukset ja organisaation toiminnan,
- ohjata tietoturvatoimintaa organisaation eri osissa.

Tietoturvaryhmän jäsenet tulisi valita organisaation omista tarpeista lähtien. Ryhmässä voi olla mukana toiminnasta vastaavien lisäksi henkilöitä esim.
- tietohallinnosta,
- laatuyksiköstä,
- riskienhallinnasta,
- viestinnästä,
- kiinteistöyksiköstä,
- henkilöstöyksiköstä,
- palvelutuotannosta ja
- valmiusyksiköstä.

Tietoturvallisuuden ohjausryhmä

Tietoturvallisuuden hallinnalla tulee olla johdon tuki. Tietoturvallisuuden ohjaukseen voidaan perustaa tietoturvallisuuden ohjausryhmä.

Organisaation ylimmästä johdosta koostuvan tietoturvallisuuden ohjausryhmän tehtävänä voi olla esim.

- hyväksyä tietoturvaperiaatteet,
- vahvistaa tietoturvallisuuden ylläpito- ja kehittämissuunnitelma,
- vahvistaa tietoturvallisuuden kehitysohjelma,
- hyväksyä auditoinnit,
- vahvistaa tietoturvallisuuden ja riskienhallinnan päälinjaukset,
- vastata tietoturvallisuuden ja riskienhallinnan toteutumisesta,
- sisällyttää tietoturvallisuuden osaksi johtamistoimintaa,
- varmistaa riittävät resurssit tietoturvallisuuden toteutumiselle,
- asettaa vaatimukset raportoinnille,
- asettaa vaatimukset tietoturvallisuuden ja riskienhallinnan huomioon ottamisesta toiminnoissa.

Tietoturvallisuuden organisointi

Tietoturvallisuuden avainroolit on syytä tunnistaa. Vastuun lisäksi henkilöllä tulee olla riittävät valtuudet tehtävän hoitamiseksi. Alla olevan taulukon avulla voidaan yksinkertaisesti kuvata avainroolit.

Rooli	Tietoturvapäällikkö
Vastuuhenkilö	N.N.
Vastuulla olevat tietoturvaprosessit ja toimenpiteet	Osallistuu riskienhallinta-, turvallisuuspolitiikan ja – periaatteiden sekä tietoturvapolitiikan määrittelyyn. Kehittää tietoturvallisuutta turvallisuuspolitiikan mukaisesti. Ohjaa tietoturvallisuuden käytännön toteutusta henkilöstön, toiminnan ja omaisuuden turvaamiseksi ja niihin kohdistuvien riskien hallitsemiseksi. Valvoo riskejä ja niiden hallinnan tilaa. Huolehtii henkilöstön turvallisuustietoisuuden lisäämisestä ja tietoturvakoulutuksen järjestelystä.
Tehtävään varattu työaika	Täysipäiväinen
Valtuudet	Valtuudet toimeenpanna ylläpito- ja kehittämissuunnitelman tehtävät. Valtuudet toimeenpanna tietoturvapolitiikan mukaiset tehtävät. Valtuudet toimeenpanna tietoturvallisuuden kehitysohjelman tehtävät. Valtuudet puuttua tietoturvapoikkeamiin.
Raportointi	Tietoturvapäällikkö raportoi ylimmälle johdolle
Varahenkilö	N.N.

Tietoturvallisuuden organisoinnissa ja rooleissa kannattaa huomioida tietoturvanäkökulmasta ainakin seuraavat roolit ja tehtävät:

- ylin johto,
- linjajohto,
- tietoturvapäällikkö/tietoturvavastaava,
- tietoturvallisuuden ohjausryhmän jäsenet,
- tietoturvallisuuteen liittyvien sidosryhmien edustajat,

- järjestelmien pääkäyttäjät/järjestelmistä vastaavat,
- tietohallintopäällikkö/-johtaja,
- fyysisestä turvallisuudesta vastaava,
- riskienhallinnasta vastaava,
- lakiasioista vastaava,
- hankinnoista ja kumppanuussuhteista vastaava,
- asiakasrajapinnassa toimivat henkilöt,
- henkilöstöasioista vastaava,
- arkistoinnista/pitkäaikaissäilytyksestä vastaava,
- henkilötiedoista vastaava/rekisterinpitäjä,
- järjestelmän kehittäjä,
- palvelutoimittajan työntekijät (esim. konsultit),
- työntekijä,
- auditoija/tarkastaja/kontrolleri,
- tietoturvallisuuteen liittyvien ohjeiden ylläpitäjät,
- ICT-järjestelmien häiriöiden selvittäjät ja toipumisesta vastaavat,
- laitteiden ja tietojärjestelmien muutoksista vastaavat,
- laitteiden ja tietojärjestelmien päivityksestä vastaavat,
- laite-, tietojärjestelmä-, palvelu-, ja ohjelmistoluetteloiden sekä lain mukaisten selosteiden ja kuvausten päivittäjät,
- laitteiden, rekistereiden ja tietojärjestelmien omistajat,
- tietoturvapoikkeamia käsittelevät henkilöt (ryhmä).

D2 Resursoinnin tarkistaminen ja tietoturvallisuuden sisällyttäminen taloussuunnitteluun

Tehtävät
- Tarkistetaan, onko vastuissa ja organisoinnissa riittävä kattavuus.
- Tietoturvallisuuden hallintaan ja ylläpitoon tarvittavien resurssien riittävyyden arviointi.

Vaiheen lopputulos
Yhteenveto tietoturvallisuuden hallintaan ja ylläpitoon tarvittavien resurssien riittävyydestä.

Resurssien tarkistaminen

Oppaan aikaisemmissa osissa on käsitelty tietoturvallisuuden lähtökohtia ja vastuita. Organisaatioissa on harvoin henkilöstöä, jolla on ylimääräistä aikaa, sen vuoksi riittävä resursointi on tietoinen päätös.

Riskienhallintatoimiin ja valvontaan tulee olla riittävästi resursseja. Tietoturvavastuuhenkilöiden osalta on tärkeä tarkastaa heidän riittävä ajankäyttö sekä valtuudet tehtävän hoitamiseksi. Tämä voi tapahtua esim. kehittämiskeskustelun yhteydessä.

Toiminta- ja taloussuunnittelu

Turvamekanismit tulisi mahdollisuuksien mukaan rahoittaa normaalitoiminnan eli operatiivisen toiminnan ja projektien kautta. Eli tietoturvallisuuden tulisi olla mahdollisimman luonteva osa normaalia taloussuunnittelua. Osa tietoturvallisuudesta vaatii kuitenkin merkittävämpää taloudellista panostusta ja priorisointia. Sen vuoksi tietoturvallisuus on suositeltava sisällyttää toiminta- ja taloussuunnittelun vuosikelloon. Alla on esimerkki toiminta- ja taloussuunnittelun (TTS) vuosikellosta, johon tietoturvallisuus on sisällytetty.

Ajankohta	Tietoturvatehtävät
Joulukuu Eduskunnan täysistunto hyväksyy valtion talousarvion	Tarkistetaan tietoturvallisuuden ylläpito- ja kehittämissuunnitelma sekä tietoturvallisuuden kehitysohjelma. Tietoturvaryhmä valmistelee esityksen tietoturvallisuuden kehittämiskohteista.
Joulukuu/tammikuu Ministeriöiden kehysehdotukset valtiovarainministeriölle (VM)	Tietoturvaryhmän ja johdon tapaaminen. Johto saa tietoturvallisuuden puolivuotisraportin. Se sisältää esityksen kehittämiskohteista ja kuvauksen tietoturvapoikkeamista. Johdon katselmointi
Tammikuu	Sisäinen auditointi
Helmikuu	Riskienarviointia ja riskienhallintasuunnittelua
Maaliskuu Hallituksen valtiontalouden vuosittainen kehyspäätös julkaistaan	Johto päättää seuraavan vuoden tietoturvallisuuden painopisteet.
Huhtikuu Ministeriöt laativat omat talousarvioesitykset VM:lle	Tietoturvallisuuteen liittyvien suunnitelmien päivittäminen. Yksiköiden ohjeistaminen tietoturvallisuuden huomioimisessa talousarvioesityksessä (TAE). Osastot soveltavat esityksessä tietoturvallisuuden kehitysohjelmaa ja osastokohtaista tietoturvatavoitetta.
Toukokuu Ministeriöt toimittavat TAE:t VM:lle	
Kesäkuu Yksiköt määrittelevät strategiset painopisteet.	Yksiköiden ohjeistaminen tietoturvallisuuden huomioimisessa strategisissa painopisteissä.
Heinäkuu Valtiovarainministeri päättää VM:n ehdotuksesta TAE:ksi ja se julkaistaan	
Elokuu Ministeriöiden ja VM:n neuvottelukierros VM:n ehdotuksen pohjalta Hallitus käsittelee talousarvioehdotusta budjettiriihessä ja lopuksi hyväksyy sisällön.	Tietoturvallisuuden ylläpito- ja kehittämissuunnitelman tarkistaminen. Tietoturvallisuuden kehitysohjelman tarkistaminen.
Syyskuu TAE annetaan hallituksen esityksenä eduskunnalle Eduskunnassa täysistunnon lähetekeskustelu	Tietoturvaryhmän ja johdon tietoturvatapaaminen. Johdolle esitetään tietoturvallisuuden puolivuotisraportti kehittämisehdotuksineen.
Lokakuu	
Marraskuu	Tietoturvallisuuden arviointi/auditointi.

D3 Auditoinnin, katselmointien ja mittaamisen suunnittelu

Tehtävä
Auditoinnin, katselmointien, valvonnan ja mittaamisen suunnittelu sekä kuvaaminen.

Vaiheen lopputulos
Auditointi-, katselmointi- ja mittaamisperiaatteet ja suunnitelmat.

Johdon katselmointi

Tehtävässä D4 on kuvattu tietoturvaryhmän ja johdon (tietoturvallisuuden ohjausryhmän) yhteistyökäytäntö. Tarkoituksena on raportoida johdolle säännöllisesti tietoturvallisuudesta. Tässä yhteydessä on luontevaa järjestää ns. ”johdon katselmointi”, jossa johto arvioi tietoturvatuloksia ja määrittää tietoturvapainotukset.

Johdon katselmoinnissa johto arvioi tietoturvallisuuden hallinnan soveltuvuutta, resurssien riittävyyttä ja tietoturvatoiminnan tehokkuutta. katselmointi dokumentoidaan ja tuloksia käytetään tietoturvatoiminnan kehittämiseen.

Yleistä auditoinneista, arvioinneista ja mittaamisesta

Auditointeja ja arviointeja tehdään eri tarkoituksiin. Niiden avulla voidaan arvioida ja raportoida johdolle tietoturvatavoitteiden saavuttaminen. Auditoinneissa käytetään tarvittaessa myös ulkopuolisia resursseja.

Auditoinneilla-, katselmoinneilla ja mittaamisilla voi olla esim. seuraavanlaisia tavoitteita:

- Riskienhallintatoimenpiteiden tehokkuuden ja toteutumisen varmistaminen;
- Kontrolleihin tehtävien muutosten negatiivisten vaikutusten arviointi;
- Turvallisuustoimenpiteiden vaikutusten analysointi;
- Turvallisuustavoitteiden saavuttamisen rekisteröinti;
- Vaatimusten noudattamisen seuranta suojaustason ja turvallisuusluokitusten mukaisesti;
- Johdon suorittama turvallisuusjärjestelmän toimivuuden säännöllinen tarkastaminen (esim. johdon ja tietoturvaryhmän kokouksessa);
- Johdon tekemä turvallisuusjärjestelmän soveltuvuuden, resurssien riittävyyden ja toiminnan tehokkuuden arviointi (esim. johdon ja tietoturvaryhmän kokouksessa);
- Seurantatarkastusten tulosten käyttö jatkuvaan parantamiseen.

Auditoinnista on voidaan laatia periaatetason dokumentti, joka määrittää pääperiaatteet, kuten

- auditoinnin kattavuus (esim. kriittiset osat, järjestelmämääritykset ja toteutukset, ydinprosessit, vaatimustenmukaisuus),
- auditointisykli (esim. ydintoiminnot auditoidaan kerran viidessä vuodessa),
- auditoijalta vaadittava pätevyys ja ulkopuolisten asiantuntijoiden käyttö,
- auditoinnin suunnittelu ja hyväksyminen,
- auditoinnista raportointi (mm. toiminnon tai kohteen omistajalle),
- auditoinnin dokumentointi,
- toiminta korjaavien toimenpiteiden yhteydessä (mm. seuranta) ja
- jälkiarviointi.

Auditointien tai arviointien perusteella sovittuja korjaavia toimenpiteitä tulee seurata. Toimet vastuutetaan ja niiden toteutumista seurataan jälkiarvioinnilla. Ydintoiminnot voidaan auditoida esim. neljän vuoden ajanjaksolla. Tämän lisäksi auditointeja (tekninen auditointi) on suositeltava tehdä esim. järjestelmäkehitysprojekteissa viimeistään ennen tuotantoon siirtoa.

Tietoturvallisuuden arviointia tulee tehdä tehtävään pätevöityneiden henkilöiden toimesta säännöllisesti (esim. vuosittain) ja auditointiprosessi on ainakin yleisellä tasolla kuvattu.

Hallinnolliset ja tekniset auditoinnit

Auditoinnit tulee tapahtua johdon hyväksymänä ja menettelyt tulee olla yhteisesti sovittu. Hyvin toteutettu auditointi suoritetaan yhteistyössä niiden toimijoiden kanssa, joiden vastuulla olevaa toimintaa auditoidaan. Auditoinnin tai arvioinnin tulokset raportoidaan toiminnon tai kohteen omistajalle.

Auditoinnit voidaan jakaa karkeasti hallinnollisiin ja teknisiin auditointeihin. Hallinnollisessa auditoinnissa arvioidaan, miten hyvin organisaatio on saavuttanut tietoturvatavoitteet ja miten hyvin se vastaa tietoturvavaatimuksiin.

Tekniset auditoinnit keskittyvät tutkimaan teknisten turvakontrollien toimivuutta ja järjestelmäprojekteissa toteutuksen turvallisuutta. Kehitys- tai räätälöintityön aikana on tärkeä järjestää katselmointeja tietoturvallisuuden kannalta kriittisiin osiin.

Mittaaminen ja tilastointi

Mittaamisen ja tilastoinnin lähtökohtana voidaan pitää tavoitteiden varmistamista. Esim. seuraavia asioita voidaan seurata

- varmuuskopioilta palautettavien tietojen määrä ja palautusten syyt,
- ylläpito- ja pääkäyttäjäoikeuksien määrä,
- käyttövaltuuksien poistoon kuluva aika,
- tietojärjestelmäympäristöjen tietoturvatavoitteiden toteutuminen,
- tietoturvapoikkeamien määrä,
- henkilöstön osallistuminen koulutuksiin ja
- tietoturvatyöhön käytetty aika.

D4 Yhteistyön, hankintatoiminnan ja raportointimenettelyjen suunnittelu

Tehtävä
Yhteistyön, hankintatoiminnan ja raportointimenettelyjen suunnittelu

Vaiheen lopputulokset

- Tietoturva-asioita käsittelevä yhteistyöryhmä (ellei ole jo aikaisemmin perustettu).
- Ohjeistus tietoturvallisuuden huomioimisesta kumppanuus- ja hankintatoiminnassa.
- Kuvaus raportointimenettelystä ja mallipohja sidosryhmäraporttia varten.

Toiminta verkostoissa

Tietoturvallisuuden hallinnan kannata on tärkeä tuntea yhteistyökumppanit. Tärkeimpiä ovat ne toimijat, jotka käsittelevät organisaation tietoja tai vaikuttavat muuten kriittisiin tietoresursseihin (esim. järjestelmät). Tämän lisäksi tulisi tunnistaa ne organisaatiot, jotka ovat riippuvaisia oman organisaation toiminnasta. Heille esim. ongelmatilanneraportointi voi olla tärkeää. Ainakin seuraavat verkostot kannatta kuvata:

- asiakkaat,
- palveluntuottajat,
- tärkeimmät yhteistyökumppanit ja
- toimintaa valvovat organisaatiot.

Alla on taulukko asiakkaan tietojen kuvaamiseksi (esimerkki).

Nimi	
Palvelu	
Asiakkaan yhteyshenkilö	
Organisaation oma yhteyshenkilö	
Miten usein raportoidaan, mistä, kenen toimesta	
Minkä suojaustason tietoja pääasiallisesti käsitellään, onko muuta turvallisuusluokitusta?	
Erityiset tietoturvavaatimukset	
Onko tehty turvallisuus-/tietoturvasopimus	

Alla on taulukko palveluntuottajan kuvaamiseksi.

Nimi	
Palvelu	
Palveluntuottajan yhteyshenkilö	
Oman organisaation yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Minkä suojaustason tietoja pääasiallisesti käsitellään, onko muuta turvallisuusluokitusta?	
Erityiset tietoturvavaatimukset	
Onko tehty turvallisuus-/tietoturvasopimus	

Alla on esitetty taulukko tärkeän yhteistyökumppanin kuvaamiseksi.

Nimi	
Yhteistyön tehtävä	
Kumppanin yhteyshenkilö	
Oman organisaation yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Minkä suojaustason tietoja pääasiallisesti käsitellään, onko muuta turvallisuusluokitusta?	
Erityiset tietoturvavaatimukset	
Onko tehty turvallisuus-/tietoturvasopimus	

Tietoturvallisuus hankinnoissa

Kumppanuus- ja hankintatoiminta tulee olla vastuutettu. Vastuuseen kuuluu myös tietoturvallisuuden huomioiminen yhteistyön alusta saakka. Palvelutoimittajien tietoturvavaatimukset tulisi määrittää jo hankintavaiheen alussa ja varmistaa, että ne tulee kuvattua tarjouspyyntöasiakirjoihin. Vaatimukset viimeistellään sopimusneuvotteluissa ja ne voidaan kuvata käytännön ohjeiksi ja määräyksiksi. Tietoturvavaatimukset suhteutetaan suojattavaan kohteeseen (tärkeä omaisuus) ja sen turvaamistarpeisiin. Käytännössä tämä tapahtuu helpoiten luokittelemalla kohde turvallisuustason mukaan. Turvaamistarpeita arvioitaessa kannattaa huomioida tietojen luottamuksellisuus, eheys ja saatavuusvaatimukset.

Hankinnan kannalta tärkeitä asioita:

- hankinnan suunnitelmallisuus,
- hankinnalle varataan riittävästi aikaa ja osaamista,

- tunnistetaan palveluun liittyvät tietoturvariskit ja määritetään tietoturvallisuuden painopisteet,
- palvelutoimittajalle asetetaan riittävän selkeät tietoturvavaatimukset,
- oma ympäristö ja sen kriittisyys tunnetaan ja
- ympäristö riittävästi dokumentoitu.

Tietoturvallisuus tarjouspyynnössä

Tietoturvallisuus voidaan sisällyttää tarjouspyyntöön kuvaamalla tietoturvatarpeet, palvelun kriittisyyden ja kuvaamalla selkeät tietoturvavaatimukset.
Tarjouspyynnössä tietoturva voidaan huomioida

- kuvaamalla selkeästi palvelun odotukset ja vaatimukset,
- kuvaamalla erityisesti ne tietoturvamenettelyt, joilla voi olla kustannusvaikutuksia,
- kuvaamalla palveluympäristön (vaarantamatta salassa pidettäviä tietoja),
- kuvaamalla tarjouspyynnön ja sen liitteiden salassapitovaatimukset (vaaditaan tarvittaessa salassapitositoumus),
- kuvaamalla selkeästi ehdottomat tietoturvavaatimukset (ml. jatkuvuusasiat),
- pyytämällä palvelutoimittajaa kuvaamaan ja tarvittaessa perustelemaan palvelun ratkaisut (tietoturvakuvaus on tärkeä),
- antamalla ohjeet, miten tarjoaja kuvaa palvelun (helpottaa tarjousten vertailua),
- mahdollistamalla auditoinnin ennen sopimuksen allekirjoittamista,
- mahdollistamalla turvallisuusselvitysmenettelyn tarvittaessa ja
- esittämällä tarvittaessa rajoitukset palvelun tuottamisesta (esim. sijaintimaa).

Tarjouspyyntöön voidaan tarvittaessa liittää luonnos turvallisuussopimuksesta. Turvallisuussopimuksen liitteenä voi olla tietoaineistojen käsittelyohje sekä muita organisaatiolle tärkeitä ohjeita tai määräyksiä.

Turvallisuussopimus

Turvallisuussopimuksen menettelyillä voi olla merkitystä palvelun tuotantokustannuksiin. Sen vuoksi sen voi sisällyttää tarjouspyyntöön. Muussa tapauksessa turvallisuussopimuksen vaatimukset on voidaan kuvata selkeästi ehdottomina vaatimuksina.

Turvallisuussopimuksessa voidaan käsitellä seuraavia asioita:

- Turvallisuussopimuksen tarkoitus ja lainsäädännöllinen viitekehys
- Turvallisuusjärjestelyt
    - Salassapito
    - Pääsy järjestelmiin
    - Palvelutuotantotilat
    - Henkilöstö (ml. turvallisuusselvitykset, koulutus, ohjeistus ja ohjaus)
    - Tietoturvallisuuden valvonta sekä poikkeamien kirjaaminen ja raportointi
    - Toimiminen asiakkaan tiloissa (esim. kulkukortit, vierailijakortit)
    - Turvallisuuden tarkastaminen ja valvonta
- Turvallisuustason seuranta
- Yhteyshenkilöt
- Turvallisuussopimuksen päivittäminen ja muuttaminen
- Sopimussakko
- Vahingonkorvausvelvollisuus
- Rikosoikeudellinen vastuu
- Sopimuksen irtisanominen ja purkaminen
- Menettelyt sopimuksen päättyessä
- Sovellettava laki ja erimielisyyksien ratkaisu
- Turvallisuussopimuksen voimassaolo

Turvalliset käytännöt

Turvallisuussopimuksen lisäksi palvelutoimittajan kanssa kannattaa sopia käytännöistä. Mikäli menettelyllä on kustannusvaikutuksia, palvelutoimittaja veloittaa siitä usein erikseen. Sen vuoksi kaikki tällaiset menettelyt kannattaa pyrkiä kuvaamaan tarjouspyynnössä.

Tärkeitä yhteisesti sovittavia menettelyjä ovat

- toimiminen tietoturvapoikkeamatilanteissa (ml. tiedottaminen, häiriöiden kirjaaminen),
- poikkeamien raportointi,
- jatkuvuuden testaaminen ja harjoittelu,
- raportointisuhteet,
- varahenkilöjärjestelyt,
- muuttuneista ohjeista ja – käytännöistä tiedottaminen,
- valvontamenettelyt,
- pääsyoikeuksien antaminen tietoon ja tiloihin,
- hankkeiden henkilöstöstä pidetään luetteloa,
- menettelytapa henkilöstössä tapahtuvien muutosten ilmoittamiseksi ja yhteyshenkilön yhteystietojen ajantasaisuus.

Sisäinen raportointi

Tietoturvallisuudesta vastaavan tulee voida raportoida suoraan ylimmälle johdolle. Sen tarkoituksena on varmistaa, että organisaation johdossa on ajantasainen tieto tietoturvatasosta. Suoran raportoinnin lisäksi johdolle laaditaan määrämuotoisia tietoturvaraportteja esim. puolivuosittain.

Esimerkki johdon puolivuotisraportin sisällöstä:

- Ajankohtaista tietoturvallisuudesta
    - trendit, organisaation toimintaa koskevat säädökset ym. (lyhyesti, mitä ne merkitsevät organisaation kannalta)
    - merkittävät tietoturvallisuuden kannalta tapahtuneet muutokset
- Tietoturvatavoitteiden toteutuminen (Miten hyvin on saavutettu ne tavoitteet, jotka on määritetty. Huom. mittarit/seurantakohteet on suositeltava määrittää etukäteen.)
- Havaitut kehittämiskohteet ja näihin liittyvät välittömät korjaavat toimenpiteet
- Kehittämisehdotukset alustavine kustannus- ja työmääräarvioineen (millä ennaltaehkäistään ongelmia, korjataan havaittuja puutteita ja kehitetään tietoturvallisuutta).

Raportointi tietoturvapäällikölle

Tietoturvapäällikkö/-vastaava priorisoi työtehtäviään ja tietoturvatilanteella on merkitystä tärkeysjärjestykseen. Vakavista tietoturvatapahtumista tulisi raportoida tietoturvapäällikölle viivytyksettä, vaikka varsinaista ongelmatilanteen hoidosta vastaisikin muu organisaatio.

Yksinkertaistetusti voidaan sanoa, että tietoturvapäällikkö tarvitsee organisaatiosta vähintään samaa tietoa, mistä se raportoi johdolle (ks. johdon puolivuotisraportti).

Ulkoinen raportointi

Ulkoista raportointia varten on tärkeä tunnistaa kontaktipisteet ja sopia menettelyistä sidosryhmien kanssa. Esimerkki asiakkaan tietoturvaraportista:

- Ajankohtaista tietoturvallisuudesta (trendit, palveluihin liittyvät säädökset ym.)
- Tietoturvatavoitteiden toteutuminen (kerrotaan lyhyesti, miten hyvin palvelussa on saavutettu yhdessä sovitut tietoturvatavoitteet)
- Havaitut kehittämiskohteet ja näihin liittyvät välittömät korjaavat toimenpiteet
- Tietoturvallisuuteen liittyvät kehittämishankkeet (miten tietoturvallisuutta on kehitetty.)

- Kehittämisehdotukset alustavine kustannus- ja työmääräarvioineen (millä ennaltaehkäistään ongelmia, korjataan havaittuja puutteita ja kehitetään tietoturvallisuutta).

D5 Tietoturvallisuuden hallinnan dokumentoinnin sekä tiedottamisen suunnittelu

Tehtävä
Tietoturvallisuuden hallinnan dokumentoinnin ja tiedottamisen suunnittelu.

Vaiheen lopputulos
Suunnitelma tai kuvaus tietoturvallisuuden hallinnan dokumentoinnista ja tiedottamisesta.

Tietoturvakäsikirja

Tietoturvallisuuden hallintakokonaisuus voidaan kuvata tietoturvakäsikirjaksi. Käsikirjan ei tarvitse olla yksi dokumentti, vaan se voi olla sähköisessä muodossa oleva, rakenteinen kokonaisuus.

Tietoturvakäsikirjan sisältö voi olla esim. seuraavanlainen:

- Käsikirjan tarkoitus ja rakenne
- Tietoturvatoimintaa ohjaavat tekijät
  - Tietoturvatoimintaa ohjaavat säädökset
  - Työjärjestys
  - Tietoturvapolitiikka
  - Tietoturvakäytännöt ja periaatteet
  - Tietoturvallisuuden kehitysohjelma
  - Tulosohjaus
- Tietoturvallisuuden organisointi
  - Tietoturvallisuuden avainroolit
  - Tietoturvallisuuden ohjausryhmä
  - Tietoturvaryhmä
  - Tietoturvavastuut ja tehtävät
- Tietoturvallisuuden sidosryhmät ja yhteistyö
  - Sisäinen tietoturvayhteistyö
  - Ulkoinen tietoturvayhteistyö
- Tietoturvallisuus hankittavissa palveluissa
  - Tietoturvallisuus hankintamenettelyissä
  - Palvelutoimittajien hallinta
- Tietoturvallisuus tuotettavissa palveluissa
- Tietoturvallisuuden ylläpito ja kehittäminen
  - Tietoturvallisuuden vuosikello
  - Tietoturvallisuuden ylläpito- ja kehittämissuunnitelma
- Seuranta, valvonta ja auditointi
  - Auditointi, katselmointien ja mittaamisen suunnittelu
  - Auditointi- ja arviointiperiaatteet
- Tärkeiden toimintojen, tieto-omaisuuden ja turvakontrollien hallinta
  - Asiakirjaturvallisuus
  - Tekniset ja fyysiset turvajärjestelyt
- Tietoturvaraportointi
  - Raportointi johdolle
  - Raportointi sidosryhmille
- Henkilöstön koulutus, ohjaus ja tuki
  - Perehdyttäminen
  - Osaamiskartoitus
  - Koulutus
  - Kannustaminen ja motivointi
  - Tietoturvallisuuden ohjeistus ja turvalliset käytännöt

    - Turvallisuusselvitykset
- Riskienhallinta ja jatkuvuuden varmistaminen
    - Riskienhallinta
    - Ennalta ehkäisevä toiminta
    - Toiminnan ja jatkuvuuden varmistaminen
    - Toipumis-, jatkuvuus- ja valmiussuunnitelmat
    - Tietoturvapoikkeamien käsittely
- Tietoturvadokumentaatio ja sen julkaisu.

Dokumentoinnin vastuuhenkilöt

Dokumentoinnissa on tärkeä löytää vastuuhenkilöt tai omistajuus ainakin

- laite-, tietojärjestelmä-, palvelu-, ja ohjelmistoluetteloiden ylläpitoon,
- lain mukaisten selosteiden ja kuvausten päivitykseen,
- turvallisuuskoulutuksen rekisteröintiin,
- seurantatarkastusten ja tietoturvatavoitteiden saavuttamisen dokumentointiin sekä
- dokumenttien säännölliseen katselmointiin.

Dokumenttien merkitseminen

Tietoturvadokumenttien hallintaa helpottaa kuvailutietojen, jakelun ja muutosmerkintöjen käyttö. Alla on esimerkki kuvailutaulukosta. Se voidaan sijoittaa esim. dokumentin kansilehdelle.

Kuvailutiedot		Päivämäärä	Allekirjoitus
Laatija			
Tarkastaja			
Hyväksyjä			
Versio nro			
Tiedoston nimi			
Suojaustasoluokitus			
Tallennuspaikka			
Omistaja			
Avainsanat			

Tietoaineistojen turvallisesta käsittelystä on kirjoitettu VAHTI 2/2010 –ohjeessa. Se on tallennettavissa valtiovarainministeriön Internet –sivuilta.

D6 Henkilöstön koulutuksen, ohjauksen ja tuen suunnittelu

Tehtävä
Henkilöstön koulutuksen suunnittelu, henkilöstöturvallisuuden varmistaminen, riittävän ohjeistuksen varmistaminen.

Vaiheen lopputulokset

- Työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti.
- Henkilöstön koulutussuunnitelma.
- Koulutusrekisteri.
- Suunnitelmat ja ohjeistot henkilöstöturvallisuuden ylläpitoon sekä parantamiseen.

Henkilöstön perehdytys ja koulutus

Tietoturvallisuus tulee huomioida jo siinä vaiheessa, kun uusi henkilö perehdytetään tehtäviin ja organisaation toimintaan. Perehdytystyötä helpottaa kirjallinen lista läpikäytävistä asioista. Henkilöstön koulutuksen suunnittelussa on tulisi kiinnittää huomiota havaittuihin riskeihin ja koulutuksessa on syytä painotta vaatimusten tärkeyttä ja oikeita toimintatapoja.

Ainoastaan säännöllinen koulutus varmistaa, että henkilöstö pysyy ajan tasalla tietoturva-asioista. Koulutuksen pääasiallinen sisältö tulisi suunnitella osana muuta koulutussuunnittelua esim. vuodeksi eteenpäin. Koulutuksen riittävää taso tulee varmistaa, esim. tekemällä osaamiskartoituksia.

Henkilöstön tulee tuntea toimintaansa kohdistuvat tärkeimmät vaatimukset sekä tietää, miten toimii toteutuneissa tai potentiaalisissa ongelmatilanteissa. Koulutuksessa on hyvä huomioida toteutuneet riskit ja käyttää paljon käytännön esimerkkejä. Myös toiminnan muutokset on hyvä huomioida. Esim. kannettavien tietokoneiden varkauksien lisääntyminen voi olla tarpeellista mainita. Hyvistä tietoturvateoista voidaan mainita koulutuksissa. Ne antavat hyvää esimerkkiä muille.

Koulutuksiin osallistumista on suositeltava seurata ylläpitämällä koulutusrekisteriä. Henkilöstön kouluttautuminen voi olla yksi tietoturvallisuuden hallinnan mittareista. Turvallisuuskoulutusta tulee arvioida tarvittaessa myös rooleittain, jolloin varmistetaan, että turvallisuudesta vastaavilla on tehtäviinsä riittävä osaaminen. Tällaista tarkastelua voidaan tehdä esim. tavoitekehityskeskustelun tai turvaluokitellun hankkeen yhteydessä. Turvallisuusluokitelluista hankkeista tulee lisäksi ylläpitää osallistujalistaa.

Ohjeistus

Muuttuneista tietoturvaohjeista ja – käytännöistä tulee tiedottaa kaikille tarvittaville osapuolille. Henkilöstössä tapahtuvista muutoksista, kuten yhteyshenkilöistä ja näiden yhteystiedoista tulee ilmoittaa niille, joita asia koskee.

Ohjeistus on suositeltava laatia ainakin seuraaviin osa-alueisiin:

- Ulkopuolisten työntekijöiden ja vierailijoiden tunnistaminen;
- Miten tunnistaa tietoturvariskit;
- Miten tunnistaa haittaohjelmia levittävät sähköpostit ja miten toimia tietoturvaongelmatilanteessa;
- Laitteiden ja järjestelmien käyttösäännöt;
- Tietoaineistojen turvallinen käsittely;
- Tietojen luokittelu;
- Salassa pidettävien manuaalisten tai siirrettävillä tietovälineillä olevien tietojen turvallinen säilyttäminen;
- Luottamuksellisten tietojen turvallinen hävittäminen;
- Salassa pidettävän tietoaineiston turvallinen kopiointi ja tulostus;
- Salassa pidettävän aineiston turvallinen sähköinen välitys;
- Salassa pidettävän aineiston turvallinen välitys postilla ja/tai kuriirilla;
- Salassa pidettävien aineistojen välityksen seuranta;
- Asiakirjojen hyväksyminen, katselmointi;
- Tietoturvavastuut, velvollisuudet, tietoturvatehtävät, työntekijän oikeudet;
- Tietoturvamääräysten ja – ohjeiden noudattamisen valvonta ja rikkomisen seuraukset;
- Turvallisuuden organisointi.

Henkilön työhönoton turvallisuusmenettelyt

Työhönottotilanteessa on syytä kiinnittää huomiota työhön otettavan osaamiseen ja luotettavuuteen. Keskeinen osaaminen voidaan todentaa koulutusdokumentaation avulla. Työhaastattelussa saatuja tietoja voidaan tarkistaa esim. pistokoemaisesti soittamalla

edellisille työnantajille. Uusien henkilöiden kohdalla on suositeltava käyttää koeaikamenettelyä.

Erityistä luotettavuutta vaativissa tehtävissä voidaan harkita turvallisuusselvitysmenettelyn ja taustojen selvittämisen tarvetta (esim. yrityskytkennät). Huumausainetestauksen käytön arviointi ja käyttömahdollisuus voidaan myös arvioida. Organisaatiossa tulisi olla määritelty ne tehtävät ja roolit, joista tehdään turvallisuusselvitykset.

Työsopimukseen voidaan liittää salassapitositoumus. Työsopimuksen yhteydessä voidaan tarvittaessa sopia sähköpostien käsittelystä poissaolojen aikana. Mikäli toimintaan, laitteisiin tai järjestelmiin liittyy erityisiä tietoturvavastuita, voidaan laatia erillinen tietoturvasitoumus, johon kuvataan tietoturvallisuuden tärkeimmät periaatteet.

Esimiehen tehtävät

Esimiehille tulee opastaa, miten toimia henkilöstössä tapahtuvissa muutostilanteissa (ilmoittaminen, käyttö- ja kulkuoikeudet). Esimiesten roolia esimerkkinä on myös syytä korostaa. Esimiesten tulisi myös tunnistaa vastuualueensa avainhenkilöt ja varmistaa varahenkilöt. Samoin hänellä tulee olla ohjeet, miten toimia työntekijän käyttäytymisen muuttuessa.

Esimies ja alainen tulisi käydä vuosittain keskustelun työn tietoturvavastuista ja osaamisen kehittämisen tarpeista (voidaan yhdistää tavoitekehityskeskusteluun). On tärkeää, että henkilöstön työtyytyväisyydestä ja työmotivaatiosta huolehditaan. Työssä jaksamisen ja työkyvyn seuranta vähentävät vahinkojen määrää.

D7 Tietoturvapolitiikan päivittäminen, hyväksyttäminen ja julkaisu

Tehtävä
Tietoturvapolitiikan viimeistely, hyväksyttäminen ja julkaisu. (Ellei ole jo aikaisemmin tehty)

Vaiheen lopputulos
Hyväksytty ja julkaistu tietoturvapolitiikka

Tietoturvapolitiikkaa on käsitelty kohdassa B5. Tässä vaiheessa sitä voidaan tarvittaessa tarkentaa ja täydentää. Tietoturvapolitiikka julkaistaan, mikäli sitä ei ole tehty aikaisemmin. Tietoturvapolitiikkaa tulee tarkastaa vuosittain.

D8 Tietoturvallisuuden ylläpito- ja kehittämissuunnitelman laatiminen

Tehtävät
- Tietoturvallisuuden ylläpito- ja kehittämissuunnitelman laatiminen ja hyväksyttäminen.
- Viimeistellään vaiheessa C5 aloitettu soveltamissuunnitelma.

Vaiheen lopputulokset
- Tietoturvallisuuden ylläpito- ja kehittämissuunnitelma. Suunnitelmassa ilmenee kertaluonteiset ja jatkuvat tehtävät esim. vuoden jaksolle.
- Valmis soveltamissuunnitelma.

Tämä on tietoturvallisuuden hallintaprojektin viimeinen tehtäväkokonaisuus. Tietoturvallisuuden ylläpito- ja kehittämissuunnitelma ohjaa jatkossa vuosittaista käytännön tietoturvatyötä ja turvakontrollien käyttöönottoa. Tietoturvallisuuden kehittämistyötä

voidaan jatkossa tehdä ja tarvittaessa projektoida pienempinä kokonaisuuksina. Kun tietoturvallisuuden ylläpito- ja kehittämissuunnitelma tarkistetaan tietoturvallisuuden ohjausryhmässä säännöllisesti, esim. alkusyksystä ja alkukeväästä, varmistetaan suunnitelmien huomioiminen budjetoinnissa. Pitkän tähtäimen tietoturvasuunnittelua ohjataan tietoturvallisuuden kehitysohjelman (tietoturvastrategia) avulla. Siitä kerrotaan tarkemmin osassa F.

E Tietoturvallisuuden fyysiset ja tekniset järjestelyt

Johdanto

Fyysiset ja tekniset turvajärjestelyt perustuvat lakiin, sopimusten kautta tuleviin vaatimuksiin sekä riskienarviointiin. Tietoaineistojen luokituskäytäntö helpottaa turvajärjestelyiden suunnittelua.

Kiinteistö- ja toimitilaturvallisuus

Uudisrakennushankkeissa ja remonteissa kannattaa tietoturvavaatimuksille varata oma tarkastelu. Vaatimustenmäärittelyä varten voidaan pohtia:

- Mikä tärkeää tieto-omaisuutta kiinteistössä on?
- Kohdistuuko tieto-omaisuuteen tiettyjä velvoitteita, kuten kansallisia tai kansainvälisiä tietojenkäsittelyvaatimuksia?
- Onko kiinteistössä/tiloissa sellaisia ominaispiirteitä, jotka altistavat tietoturvaongelmille?
- Minkä suojaustason tietoja tiloissa pääasiallisesti käsitellään?
- Voidaanko korkeamman suojaustason tietojen käsittely keskittää tiettyihin tiloihin?
- Liikkuuko tiloissa ulkopuolisia?

Mikäli organisaatio luokittelee tietoaineistoja, se voi soveltaa suunnittelussa KATAKRIa (Kansallinen auditointikriteeristö).

Rakennushankkeen suunnittelutyö kannattaa tehdä yhteistyössä arkkitehdin kanssa. Tarvittaessa voidaan käyttää ulkopuolista turvallisuusasiantuntijan apua.

Kiinteistön ympäristössä on syytä arvioida tarve:

- Alueen videovalvonnalle;
- Varautuminen salakuunteluun kiinteistön alueella tapahtuvan liikkumisen rajoittamisella;
- Hajasäteilyyn ja vastaaviin uhkiin varautumiselle.

Kiinteistössä on suositeltava varmistaa riittävät

- kuoren rakennemateriaalit ja aukkojen suojaaminen,
- ovien murtosuojaus,
- rikosilmoitinjärjestelmä,
- kulunvalvontajärjestelmä,
- kameravalvontajärjestelmä,
- ikkunoiden sijainti maantasoon nähden,
- kattoikkunoiden suojaus,
- LVIS-järjestelmien kapasiteetti ja turvallisuus,
- turvallinen avaintenhallinta ja tilojen pääsyoikeuksien hallinta,
- yleisavaimen pääsyrajoitukset,
- vartiointi- ja kiinteistönhoitohenkilöstön avaintenhallinta,
- vyöhykeperiaate ja
- piha-alueen turvallisuus.

Tiloissa huomioitavaa:

- näyttöpäätenäkymän suojaaminen,
- äänieristys,
- lukitus,
- avaintenhallinta ja pääsyoikeuksien hallinta,
- kassakaapit ja holvit voivat vaatia erityisiä rakenteita,
- huoltotoimenpiteiden järjestäminen valvotusti,
- kulkukorttien käyttö,
- vierailijakäytäntö ja
- järjestelmien säännöllinen toimintavarmuuden testaus.

Huom. IT- ja laitetilat tulee suunnitella erikseen.

Tietojärjestelmäturvallisuus

Tietojärjestelmäturvallisuus perustuu järjestelmien elinkaaren hallintaan, turvallisiin kuvattuihin menettelytapoihin ja toipumisvalmiuteen. Tietoturvallisuuden tulee olla osa järjestelmäkehitystä.

Perusasioita tietojärjestelmäturvallisuuden varmistamiseksi ovat

- riskianalyysi
- tietojärjestelmien kriittisyysluokitus,
- vastuut ja organisointi kehitys- ja ylläpitotehtäviin,
- riittävä ohjeistus ja niiden päivittäminen,
- ongelmatilanteiden hallintamenettelyt,
- verkon, järjestelmien ja niiden käytön valvonta,
- teknisen ympäristön riittävä dokumentointi ja niiden varmistus (ml. konfigurointitiedot),
- muutoshallinta- ja hyväksymismenettelyt,
- tietoliikenneverkon rakenteen turvallisuus ja tietoliikenteen turvallinen ylläpito,
- laitteiden koventaminen,
- käyttäjien tunnistaminen ennen pääsyn sallimista järjestelmiin ja palveluihin,
- laitteiden ja järjestelmien päivitys,
- suojautuminen haittaohjelmia vastaan,
- lokimenettelyt,
- salausratkaisut ja salausavainten hallinta,
- istunnonhallinnan turvallinen toteuttaminen,
- autentikaatiodatan suojaaminen tietojärjestelmissä,
- ohjelmistojen, tietoliikenneyhteyksien ja oheislaitteiden asentamiseen liittyvät periaatteet,
- kehitys-/testaus- ja tuotantojärjestelmien erottaminen,
- tunnettujen haavoittuvuuksien estäminen verkoissa ja sen palveluissa,
- vaarallisten työyhdistelmien välttäminen,
- riittävästä varmuuskopioinnista ja suojakopioinnista huolehtiminen,
- toipumissuunnitelmat kriittisiin järjestelmiin ja niiden testaaminen.

Seuraavien käytäntöjen tarvetta voidaan arvioida:

- Ylläpito- ja pääkäyttäjäoikeuksien määrän seuranta ja tilastointi.
- Käyttövaltuuksien poistoon kuluvan ajan seuranta ja tilastointi.
- Menettelyt tietoturva- ja korjauspäivityksiin.
- Tärkeimpiin tietojärjestelmiin laaditaan toipumissuunnitelmat ja toipumisvalmiutta testataan säännöllisesti.
- Menettelyt liikuteltavien tietovälineiden suojaamiseksi luvatonta pääsyä ja käyttöä vastaan.
- Ajettavan koodin turvallisuuden varmistaminen.
- Periaatteet ja mekanismit etä- ja matkatöiden riskien hallitsemiseksi.

F Tietoturvallisuuden kehitysohjelma ja jatkuva kehittäminen

Tietoturvallisuuden kehitysohjelma (tietoturvastrategia)

Tietoturvallisuuden kehitysohjelma on strategiatason kirjallinen suunnitelma, josta käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi. Kehitysohjelma on suositeltava laatia usean vuoden ajanjaksolle ja sitä tulisi tarkistaa aina, kun tietoturvallisuuden strategisia linjauksia muutetaan. Tietoturvallisuuden kehitysohjelmasta käytetään myös nimitystä “tietoturvastrategia”

Tietoturvallisuuden ylläpito- ja kehittämissuunnitelma ohjaa käytännön tietoturvallisuuden kehittämistyötä. Suunnitelmaa on käsitelty tehtävässä D8.

Tietoturvallisuuden jatkuva kehittäminen

Oppaan alussa on tiivistelmä eri tehtävistä ja lopputuloksista. Alla olevassa taulukossa on esitetty, millainen taulukko voi olla, kun tietoturvallisuuden kehittäminen on jatkuvaa toimintaa. Eri osa-alueista voi laatia ”tietoturvallisuuden vuosikellon” kohdassa D2 esitetyn TTS-suunnitelman tietoturvallisuuden vuosikellon mukaisesti.

Vaihe	Tärkeimmät tehtävät	Tärkeimmät lopputulokset
A1 Tietoturvallisuuden lähtökohtien määrittäminen ja kuvaaminen	Tietoturvavaatimusten tarkistaminen Tietoturvatavoitteiden tarkistaminen ja tarvittaessa päivittäminen	Lyhyt yhteenveto tietoturvallisuuden kannalta merkittävistä vaatimuksista Kuvaus organisaation tietoturvatavoitteista Suunnitelma tietoturvavaatimusten ja tavoitteiden kohdistamisesta (voidaan sisällyttää ylläpito- ja kehittämissuunnitelmaan)
A2 yhdistyy tehtävään B1	Ks. B1	Ks. B1
A3 yhdistyy tehtävään D1	Ks. D1	Ks. D1
A4 yhdistyy tehtävään D8	Ks. D8	Ks. D8
A5 yhdistyy tehtävään D4	Ks. D4	Ks. D4
B1 Tietoturvallisuuden hallinnan kattavuuden ja riippuvuuksien määrittäminen	Tarkistetaan kuvaukset tärkeimmistä sidosryhmistä ja riippuvuuksista Tarkistetaan, kattaako tietoturvallisuuden hallinta toimintaa riittävästi	Ajantasainen kuvaus tärkeimmistä tietoturvallisuuden sidosryhmistä ja riippuvuussuhteista Ajantasainen kuvaus tietoturvallisuuden hallinnan kattavuudesta
B2 Tärkeiden toimintojen, tietoomaisuuden ja turvakontrollien kuvaaminen	Tarkistetaan tärkeiden toimintojen ja tietoomaisuuden kuvaukset. Täydennetään tarvittaessa. Tarkistetaan turvajärjestelyiden (turvakontrollien) kuvaukset. Päivitetään ja täydennetään tarvittaessa.	Kuvaus organisaation tärkeimmistä toiminnoista, suojattavista kohteista ja näihin liittyvistä turvakontrolleista

B3 Teknisen ja fyysisen tietojenkäsittely-ympäristön kuvaaminen	Tärkeitä toimintoja tukevan teknisen ja fyysisen tietojenkäsittely-ympäristön kuvaaminen Tärkeiden resurssien teknisten turvakontrollien kuvaaminen	Kuvaus tai kooste teknisestä ja fyysisestä tietojenkäsittely-ympäristöstä turvajärjestelyineen.
B4 Tietoturvallisuuden nykytilanteen ja vaatimustenmukaisuuden arviointi	Sisäinen auditointi/arviointi Tietoturvallisuuden nykytilanteen sekä vaatimustenmukaisuuden arviointi ja raportointi johdolle.	Auditointiraportti Arvio siitä miltä osin tietoturvallisuutta tulee organisaation tarpeisiin, toimintoihin ja suojattaviin kohteisiin nähden parantaa.
B5 Tietoturvapolitiikan päivitys tai laatiminen	Tietoturvapolitiikan tarkistaminen ja tarvittaessa päivittäminen.	Ajantasainen, johdon hyväksymä tietoturvapolitiikka
C1 Riskienhallinta- ja häiriötilannehallintamenettelyjen määrittäminen sekä kuvaaminen	Riskienhallinta- ja häiriötilannemenettelyjen tarkistaminen.	Ajantasainen ja tarvittaessa täydennetty kuvaus riskienhallinta- ja häiriötilannemenettelyistä.
C2 Riskien tunnistaminen ja analysointi	Riskien tunnistaminen ja analysointi Arvioidaan ja valitaan riskienhallintatoimet	Riskianalyysi
C3 Riskienhallinta-toimenpiteiden suunnittelu ja turvakontrollien valinta	Riskienhallinnan suunnittelu ja turvakontrollien valinta. Jäännösriskien arviointi.	Riskienhallintasuunnitelma ja kuvaus valituista turvakontrolleista. Riskienhallintasuunnitelma voidaan sisällyttää tietoturvallisuuden ylläpito- ja kehittämissuunnitelmaan (ks. D8).
C4 Jäännösriskien ja tärkeimpien turvakontrollien hyväksyttäminen johdolla	Hyväksyttävän riskitason päättäminen. Tietoturvallisuuden jäännösriskien hyväksyttäminen johdolla	Merkintä tai hyväksymispöytäkirja
C5 Tietoturvallisuuden viitekehyksen valinta, soveltamissuunnitelman laatiminen	Soveltamissuunnitelman laatiminen valitun viitekehyksen mukaan	Soveltamissuunnitelma (voi olla useita)
D1 yhdistyy tehtävään D2	Ks. D2	
D2 Resursoinnin tarkistaminen ja tietoturvallisuuden sisällyttäminen taloussuunnitteluun	Tarkistetaan, onko vastuissa ja organisoinnissa riittävä kattavuus. Tietoturvallisuuden hallintaan ja ylläpitoon tarvittavien resurssien riittävyyden arviointi. Tietoturvallisuuden budjetointi ja organisaation tukeminen taloussuunnittelussa	Yhteenveto tietoturvallisuuden hallintaan ja ylläpitoon tarvittavien resurssien riittävyydestä. Ajantasainen ja tarvittaessa täydennetty kuvaus tietoturvallisuuden organisoinnista, rooleista, vastuista sekä valtuuksista. Riittävä tietoturvaorganisaatio Tietoturvallisuuden sisältyminen budjettiin ja taloussuunnitteluun.

D3 Auditoinnin, katselmointien ja mittaamisen suunnittelu	Auditoinnin, katselmointien, valvonnan ja mittaamisen suunnittelu.	Suunnitelma auditoinneista, katselmoinneista, valvonnasta ja mittaamisesta vuodeksi eteenpäin.
D4 Yhteistyön, hankintatoiminnan ja raportointimenettelyjen suunnittelu	Tietoturvayhteistyön riittävyyden arviointi Tietoturva-asioita käsittelevä yhteistyöryhmän kokoonpanon tarkistaminen Johdon yhteistyömenettelyn tarkistaminen Hankintatoiminnan ohjeistuksen ja riittävän ohjauksen tarkistaminen Raportoinnin riittävyyden tarkistaminen. Johdon yhteistyökokoukset Johdon katselmointi	Johdon raportti Johdon katselmointiyhteenveto Kokouspöytäkirjat Päätökset tietoturvallisuuden painopisteistä
D5 Tietoturvallisuuden hallinnan dokumentoinnin sekä tiedottamisen suunnittelu	Tietoturvallisuuden hallinnan dokumentoinnin ja tiedottamisen suunnittelu.	Ajantasainen suunnitelma tai kuvaus tietoturvallisuuden hallinnan dokumentoinnista ja tiedottamisesta.
D6 Henkilöstön koulutuksen, ohjauksen ja tuen suunnittelu	Henkilöstön koulutuksen suunnittelu, henkilöstöturvallisuuden varmistaminen, riittävän ohjeistuksen varmistaminen. Henkilöstökoulutusten, perehdytysten ja ohjauksen järjestäminen. Puuttuminen väärinkäytöksiin. Viestiminen tietoturvallisuudesta tarvittaville tahoille.	Henkilöstön koulutussuunnitelma. Koulutusrekisteri. Suunnitelmat ja ohjeistot henkilöstöturvallisuuden ylläpitoon sekä parantamiseen.
D7 Tietoturvaperiaatteiden päivittäminen, hyväksyttäminen ja julkaisu	Tietoturvaperiaatteiden päivittäminen, täydentäminen ja julkaisu	Ajantasaiset ja julkaistut tietoturvaperiaatteet
D8 Tietoturvallisuuden ylläpito- ja kehittämissuunnitelman laatiminen	Tietoturvallisuuden ylläpito- ja kehittämissuunnitelman päivittäminen	Päivitetty tietoturvallisuuden ylläpito- ja kehittämissuunnitelma.

Lähteet

Kuula, A. K. 1999. Toimintatutkimus, Kenttätyötä ja muutospyrkimyksiä. Tampere: Vastapaino.

ISO/IEC TR 13335-3:1998. Guidelines for the management of IT Security - Part 3: Techniques for the management of IT. Geneva: Security International organization for standardization.

ISO/IEC TR 13335-4:2000. Guidelines for the management of IT Security - Part 4: Selection of safeguards. Geneva: International organization for standardization.

ISO/IEC TR 13335-5:2001. Guidelines for the management of IT Security - Part 5: Management guidance on network security. Geneva: International organization for standardization.

ISO/IEC 27001:2005. Information security management systems – Requirements. International organization for standardization.

ISO/IEC 27000:2009. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27001:2005, Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27002:2005, Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27003:2010, Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27004:2009, Tietoturvallisuuden hallinta. Mittaaminen. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27005:2008, Tietoturvariskien hallinta. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27006:2007, Tietoturvallisuuden hallintajärjestelmien auditointi- ja sertifiointielinten vaatimukset. Helsinki: Suomen Standardoimisliitto SFS; Geneva: International organization for standardization.

ISO/IEC 27007, Tietoturvallisuuden hallintajärjestelmän auditointiohjeet.

Kallioinen, O. 2008. Oppiminen Learning by Developing –toimintamallissa. Laurea-ammattikorkeakoulu.

Kansallinen turva-auditointikriteeristö (KATAKRI), 2009. Puolustusministeriö. (Saatavana osoitteesta www.defmin.fi.)

Kuusela. Realistinen toimintatutkimus? Toimintatutkimus, työorganisaatiot ja realismi. Helsinki:2005

Ojasalo, K., Moilanen, T. & Ritalahti J. 2009. Kehittämistyön menetelmät - uudenlaista osaamista liiketoimintaan. Helsinki: WSOY pro.

Petri Puhakainen. 2006. A Design Theory for Information Security Awareness, Oulun yliopisto.

Valtiovarainministeriö. 2007. Valtionhallinnon tietoturvatasot, hankeryhmän loppuraportti. (Saavavana osoitteesta www.valtiovarainministeriö.fi)

Valtiovarainministeriö. 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010.

Valtiovarainministeriö. 2007. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan VAHTI 3/2007

Sähköiset lähteet

Arkistolaki (831/1994) 7§, 8§, 4. luku. Tulostettu 20.10.2010

Asetus tietoturvallisuudesta valtionhallinnossa (TTA, 681/2010) Tulostettu 16.8.2010

Asetus viranomaisten toiminnan julkisuudesta (1030/1999) Tulostettu 19.10.2010

Henkilötietolaki (523/1999) Tulostettu 20.10.2010

Laki turvallisuusselvityksistä (177/2002) Tulostettu 21.10.2010

Laki viranomaisten toiminnan julkisuudesta (621/1999) ja 38§:n muutos (636/2000) Tulostettu 19.10.2010

Suomen perustuslaki (731/1999) -10§ ja 12§. Tulostettu 19.10.2010

Sähköisen viestinnän tietosuojalaki (516/2004) Tulostettu 21.10.2010

Valmiuslaki (1080/1991) Tulostettu 21.10.2010

http://www.huolintaliitto.fi/ytnk08/fi/julkaisut_liitteet/KATAKRI_suositusohje_lopullinen.pdf Kansallisen turvallisuusauditointikriteeristön (KATAKRI) suositusosuuden käyttöohje

Valtiovarainministeriö. Keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004) Tulostettu 15.11.2010

Valtiovarainministeriö. Tietoturvallisuuden arviointi valtionhallinnossa (VAHTI 8/2006) Tulostettu 20.11.2010

Valtiovarainministeriö. Tietoturvallisuuden hallintajärjestelmän arviointisuositus (VAHTI 3/2003) Tulostettu 15.11.2010

Valtiovarainministeriö. Tietoturvallisuus ja tulosohjaus (VAHTI 2/2004). Tulostettu 15.11.2010

Valtiovarainministeriö. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä, VAHTI 7/2009. Tulostettu 20.10.2010

Valtiovarainministeriö. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, VM 0024:00/02/99/1998 Tulostettu 20.10.2010

VATT http://www.vatt.fi/file/vatt_publication_pdf/t159.pdf Mainettaan parempi tuottavuusohjelma? Katsaus valtion virastojen ja laitosten työn tuottavuuteen ja työhyvinvointiin

www.google.com. Hakutulos sanoilla ”tietoturvallisuuden hallinta”. Tulostettu 4.5.2011

www.google.com. Hakutulos sanoilla ”information security management”. Tulostettu 4.5.2011

Tanskan valtionhallinnossa kehitetty tietoturvastandardi http://www.itst.dk/sikkerhed/standarder/ds-484-og-iso-27002/kapitler-i-ds-484 (Poimittu 23.5.2011)

Liite 1 Oppaan tehtävien liittyminen VAHTI 2/2010 liitteen 5 tietoturvatasojen kriteereihin

Alla olevassa taulukossa on kuvattu VAHTI 2/2010 liitteessä 5 kuvatut kriteerit ja ne oppaan tehtävät, jotka liittyvät toisiinsa. Tietoturvatasokriteeristö löytyy valtiovarainministeriön Internet-sivuilta www.vm.fi (VAHTI).

1.1. Johtajuudelle asetettavat vaatimukset		
1.1.1 Strateginen ohjaus		Tehtävä
1.1.1.3. Perustaso	Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.	A1, A3, D5, D6
1.1.1.4. Perustaso	Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.	A3, B2
1.1.1.5. Perustaso	Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.	B5, D5, D7
1.1.1.6. Korot. taso	Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.	A3, A4, D5, D8, F
1.1.1.7. Korkea taso	*Organisaatiolla on vuosittainen tietoturvallisuuden kehittämissuunnitelma.*	A4, D5, D8, F
1.1.1.8. Korkea taso	*Tulosohjauksessa käytetään myös tietoturvallisuuteen liittyviä osuuksia.*	D2
1.1.2 Resursointi ja organisointi		
1.1.2.1. Perustaso	Organisaatioon on nimitetty tietoturvavastaava, jonka työnkuvassa on mainittu tietoturvavastuut.	A3, D1
1.1.2.2. Perustaso	Tietoturvavastaavalla on aikaa tietoturvavastuidensa suorittamiseen.	D2
1.1.2.3. Korot. taso	Kaikkien tietoturvavastuita omaavien työnkuvissa vastuu on mainittu.	A3, D1
1.1.2.4. Korot. taso	Organisaatiossa on sen kokoon ja tavoitteisiin nähden riittävästi tietoturvahenkilöstöä.	A3, D1, D2
1.1.2.5. Korot. taso	Tietoturvallisuuden resursointi on huomioitu organisaation toiminta- ja taloussuunnittelussa tai budjetissa ja toteutumista seurataan.	D2
1.1.2.6. Korkea taso	*Tietoturvavastaava on päätoiminen.*	*D1, D2*
1.1.3 Yhteistyön koordinointi		
1.1.3.1. Perustaso	Organisaation johto ja tietoturvallisuuden eri osa-alueiden vastuuhenkilöt keskustelevat säännöllisesti.	D4
1.1.3.2. Perustaso	Organisaatiossa on säännöllisesti kokoontuva tietoturva-asioita käsittelevä yhteistyöryhmä.	D4
1.1.3.3. Korot. taso	Johdon tapaamiset ovat vähintään kerran vuodessa.	D4
1.1.3.4. Korot. taso	Tietoturva-asioita käsittelevä yhteistyöryhmä kokoontuu vähintään kaksi kertaa vuodessa	D4
1.1.3.5. Korkea taso	*Tapaamisissa käsitellään mm. havaittuja riskejä, asetettuja tietoturvatavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia.*	*D4*
1.1.3.6. Korkea taso	*Tapaamisista pidetään pöytäkirjaa ja sovittujen toimenpiteiden toteutumista seurataan.*	*D4, D5*
1.1.4 Raportointi ja viestintä sidosryhmille		
1.1.4.1. Perustaso	Sidosryhmät, joille organisaatio on vastuussa tietoturvallisuudesta, ja niiden kontaktipisteet on tunnistettu.	D4

1.1.4.2. Perustaso	Johto on organisoinut ja vastuuttanut sidosryhmiin vaikuttavista tietoturva- asioista raportoinnin sekä tietoturvapoikkeamista tiedottamisen.	D4
1.1.4.3. Korot. taso	Sidosryhmille raportoidaan tietoturvallisuudesta vuosittain tai johdon määrittelemällä tavalla.	D4
1.1.4.4. Korot. taso	Sidosryhmäraportilla on mallipohja	D4, D5
1.1.4.5. Korkea taso	*Jos muuta ei sovita, raportin sisältöön kuuluu mittaustietoa vaatimuksenmukaisuudesta, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset.*	D4, D5
1.1.4.6. Korkea taso	*Raportointia kehitetään sidosryhmien palautteen perusteella*	D4
1.1.5 Johtaminen erityistilanteessa		
1.1.5.1. Perustaso	Tietoturvapoikkeamien käsittely on organisoitu ja vastuutettu.	A3, C1
1.1.5.2. Perustaso	Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa.	C1
1.1.5.3. Korot. taso	Organisaatiossa on kirjallinen malli tietoturvapoikkeamien käsittelyyn. Ohjeessa on määritelty roolitasolla kuka selvittää tapahtunutta kenen määräyksestä ja kuka päättää viranomaiskontakteista (esim. esitutkintapyynnön teosta) ja tiedottamisesta.	C1
1.1.5.4. Korot. taso	Tietoturvapoikkeamista tehdään jälkikäteisanalyysi ja käynnistetään tarvittavat korjaavat toimenpiteet tapahtuman uusiutumisen ehkäisemiseksi.	C1
1.1.5.5. Korkea taso	*Havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto.*	C1, D3
1.1.5.6. Korkea taso	*Tietoturvapoikkeamista vaihdetaan tietoja kumppanien kanssa ja kumppanien kokemuksia käytetään hyväksi.*	D4
1.1.6 Raportointi johdolle		
1.1.6.1. Perustaso	Tietoturvallisuudesta raportointi on vastuutettu ja organisoitu.	A3, D4
1.1.6.2. Perustaso	Tietoturva-asioista raportoidaan organisaation johdolle säännöllisesti.	D4
1.1.6.3. Korot. taso	Raportointimenettely on kuvattu kirjallisesti.	D4
1.1.6.4. Korot. taso	Tietoturva-asioista raportoidaan organisaation johdolle vähintään vuosittain	D4
1.1.6.5. Korkea taso	*Jatkuva raportointi perustuu päätettyihin toiminnan mittareihin.*	D4
1.1.6.6. Korkea taso	*Raportin sisältöön kuuluu mittaustietoa resurssien käytöstä, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset.*	D4
1.2 Toiminnan suunnittelulle asetettavat vaatimukset		
1.2.1 Toimintaympäristön vaikutus		
1.2.1.1. Perustaso	Erilliset tietojen käsittelyn toimintaympäristöt ja niihin kuuluvat järjestelmät ja toiminnot on tunnistettu.	B1, B2, B3
1.2.1.2. Perustaso	Kunkin toimintaympäristön erityisvaatimukset ja tavoitteet tietoturvallisuuden osalta on tunnistettu	A1, B2
1.2.1.3. Korot. taso	Toimintaympäristöt ja niihin kuuluvat järjestelmät on	B2, B3

	dokumentoitu.	
1.2.1.4. Korot. taso	Ympäristö- ja järjestelmälistaukset katselmoidaan ja tarvittaessa päivitetään vähintään vuosittain	B2, B3, D3
1.2.1.5. Korkea taso	*Ympäristöjen elinkaaren vaiheet on dokumentoitu ja dokumentissa on kriteerit milloin ja miten ympäristö siirtyy vaiheesta toiseen.*	B3, E
1.2.1.6. Korkea taso	*Kunkin elinkaaren vaiheen erityisvaatimukset tietoturvallisuuden osalta on määritelty ja dokumentoitu.*	B3, E
1.2.2 Tavoitteiden määrittely		
1.2.2.1. Perustaso	Kunkin ydintoiminnon ja -prosessin tietoturvallisuuden kannalta suojattavat kohteet on tunnistettu ja luokiteltu vaadittavan tietoturvallisuuden tason mukaisesti.	B2
1.2.2.2. Perustaso	Ydintoimintojen tai -prosessien tavoitteisiin on liitetty myös tietoturvatavoitteita.	A1, B2
1.2.2.3. Korot. taso	Tietoturvatavoitteiden määrittelyssä on otettu huomioon sekä luottamuksellisuus, eheys että saatavuus.	A1, B2
1.2.2.4. Korot. taso	Ydintoiminnoista ja -prosesseista on karkean tason toiminta- tai prosessikuvaukset.	B2
1.2.2.5. Korkea taso	*Toiminto- tai prosessikuvauksiin on liitetty tietoturvallisuuden kannalta oleelliset tietoturvaprosessit tai toimet tai ne on dokumentoitu erikseen.*	B2, B3
1.2.2.6. Korkea taso	*Toimintojen tietoturvatavoitteisiin on liitetty suoriutumista kuvaavia mittareita.*	A1, B2, D3
1.2.3 Toiminnan kehittäminen riskien arvioinnilla		
1.2.3.1. Perustaso	Organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia.	C1, C2, F
1.2.3.2. Perustaso	Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä.	C1, C2, F
1.2.3.3. Korot. taso	Organisaatiossa tehdään ydintoimintojen tietoturvariskien arviointia vähintään vuosittain.	C1, F
1.2.3.4. Korot. taso	Organisaatiolla on riskien arvioinnin menetelmä ja ohjeistus.	C1
1.2.3.5. Korot. taso	Organisaatiolla on kirjallinen tietoturvasuunnitelma, joka määrittelee mitä teknisiä ja hallinnollisia toimia ja prosesseja organisaatiossa käytetään havaittujen tietoturvariskien hallitsemiseksi.	C1, C2, C3
1.2.3.6. Korkea taso	*Organisaatiossa tehdään tietoturvariskien arviointia myös suurten muutosten yhteydessä*	C1, E, F
1.2.3.7. Korkea taso	*Organisaatiolla on riskienhallintapolitiikka.*	C1
1.2.3.8. Korkea taso	*Suurimmista riskeistä pidetään koko organisaation tasolla kirjaa ja riskienhallintatoimenpiteiden toteutumista seurataan.*	C1, C3, D3
1.2.4 Toimintaverkoston hallinta		
1.2.4.1. Perustaso	Organisaatiossa on tiedossa, missä toimintaverkostoissa organisaatio on mukana sekä mitä alihankkijoita ja yhteistyökumppaneita sen tietojen kanssa toimii missäkin roolissa.	B1, B2, D4
1.2.4.2. Korot. taso	Organisaatiolla on kirjallinen dokumentti, jossa kuvataan sen osallistumista ja roolia erilaisissa alihankinta- ja yhteistyöverkostoissa sekä osallistumisen yleisiä tietoturvavaatimuksia.	A1, B1, B2, D4

1.2.4.3. Korkea taso	*Toimintoverkostot on luokiteltu tietoturvatason mukaan ja kullakin luokalla on omat tietoturvavaatimuksensa.*	A1, D4
1.2.4.4. Korkea taso	*Palveluntarjoajaksi voidaan valita vain sellainen palveluntarjoaja, jolla on mahdollisuus suojata asiakirjojen luottamuksellisuus ja tarvittaessa selvittää luottamuksellisuuden loukkaukset sähköisen viestinnän tietosuojalain (516/2004) 13 a - 13k §.ssä tarkoitetulla tavalla.*	D4
1.2.5 Erityistilanteiden hallinta		
1.2.5.1. Suomen erityisv.	Organisaation johto on tiedostanut mitä yhteiskunnan elintärkeiden toimintojen turvaamiseen (YETT) liittyviä vastuita organisaatiolla on.	A1, A5, B4
1.2.5.2. Perustaso	Organisaatiolla on jatkuvuussuunnitelma tai -suunnitelmia.	C1, E, F
1.2.5.3. Korot. taso	Jatkuvuussuunnitelmien päivitys ja katselmointi on vastuutettu ja organisoitu.	A3, C1, E, F
1.2.5.4. Korot. taso	Jatkuvuussuunnitelmien toimivuutta testataan, harjoitellaan ja arvioidaan säännöllisesti.	C1, E, F
1.2.5.5. Korkea taso	*Jatkuvuussuunnitelmien toimivuutta harjoitellaan keskeisten yhteistyökumppanien kanssa.*	C1, E, F
1.3 Henkilöstölle asetettavat vaatimukset		
1.3.1 Osaamisen ja tietoisuuden kehittäminen sekä sanktiot		
1.3.1.1. Suomen erityisv.	Työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti (Laki yksityisyyden suojasta työelämässä, 21§).	A1, D6
1.3.1.2. Perustaso	Organisaatiossa järjestetään säännöllisesti tietoturvakoulutusta henkilöstölle ja muille avainryhmille. Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään.	D6
1.3.1.3. Perustaso	Perehdyttämistilanteessa käsitellään myös tietoturva-asioita.	D6
1.3.1.4. Perustaso	Muuttuneista tietoturvaohjeista ja -käytännöistä tiedotetaan kaikille organisaatiossa toimiville.	D4, D6
1.3.1.5. Perustaso	Sääntöjen noudattamista seurataan ja poikkeamiin puututaan.	D6
1.3.1.6. Korot. taso	Organisaatiossa on kirjallinen tietoturvallisuuden koulutussuunnitelma.	D6
1.3.1.7. Korot. taso	Perehdyttäjällä on kirjallinen lista käsiteltävistä tietoturva-asioista.	D6
1.3.1.8. Korot. taso	Henkilöstön osallistumista koulutuksiin seurataan.	D6
1.3.1.9. Korot. taso	Tietoturvamääräysten ja -ohjeiden rikkomisen seuraukset on kuvattu organisaatiossa ja tiedotettu kaikille organisaatiossa työskenteleville.	D6
1.3.1.10. Korot. taso	Esimies ja alainen käyvät vuosittain keskustelun työn tietoturvavastuista ja osaamisen kehittämisen tarpeista.	D6
1.3.1.11. Korot. taso	Henkilöstön tietoturvaosaamisesta varmistutaan.	D6
1.3.1.12. Korkea taso	*Tietoturvakoulutuksessa otetaan huomioon organisaatiossa ja lähiympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat.*	D6
1.3.1.13. Korkea taso	*Hyvistä tietoturvateoista annetaan positiivista huomiota.*	D6
1.3.2 Henkilöresurssien ja tehtävien hallinta		
1.3.2.1. Perustaso	Toteutettavaksi valitut tietoturvatoimenpiteet ja -	A3, A4,

	prosessit on organisoitu ja vastuutettu.	C3, D8
1.3.2.2. Perustaso	Tietoturvallisuuden avainroolit on tunnistettu ja niille on nimetty varahenkilö tai -henkilöt.	A3, D1, D2
1.3.2.3. Korot. taso	Toteutettavaksi valituista tietoturvaprosesseista tai -toimenpiteistä ja niiden vastuuhenkilöistä on luettelo.	A3, A4, C3, D8
1.3.2.4. Korot. taso	Tietoturvallisuuden varahenkilöt on koulutettu tehtäväänsä	D6
1.3.2.5. Korkea taso	*Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu.*	D6
1.3.2.6. Korkea taso	*Organisaatiossa on tehty tietoturvallisuuden osaamiskartoitus*	D6
1.3.3 Erityistilanteissa toimiminen		
1.3.3.1. Suomen erityisv.	Sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös tietoturvapoikkeamatilanteita selvitettäessä (Sähköisen viestinnän tietosuojalaki 4§ ja 5§ sekä Laki yksityisyyden suojasta työelämässä 6. luku).	A1, B4
1.3.3.2. Perustaso	Henkilöstö tietää, kenelle tietoturvapoikkeamista ja -tapahtumista tai niiden uhkista tulee ilmoittaa.	D6
1.3.3.3. Korot. taso	Tietoturvapoikkeamia selvittävät henkilöt on koulutettu tehtäväänsä.	D6
1.3.3.4. Korkea taso	*Organisaatiossa on tietoturvapoikkeamien selvittämiseen koulutettu ryhmä, joka harjoittelee säännöllisesti.*	A3, D1, D6
1.4 Kumppanuuksille ja resurssien hallinnalle asetettavat vaatimukset		
1.4.1 Sopimusten hallinta		
1.4.1.1. Perustaso	Kumppanuus- ja hankintatoiminta on vastuutettu ja organisoitu.	A3, D4
1.4.1.2. Perustaso	Kumppanin kanssa tehdään kirjallinen sopimus, jossa määritellään yhteistyön tai hankinnan kohteen tietoturvavaatimukset sekä miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.	A1, D4
1.4.1.3. Korot. taso	Kumppanille asetetaan tarvittavat tietoturvavaatimukset jo tarjouspyyntö- tai kumppanuusneuvotteluvaiheessa.	A1,D4
1.4.1.4. Korot. taso	Kumppanuussopimuksessa määritellään mitä tietoturvallisuustasoa kumppanin ja mahdollisen kumppanin alihankintaverkoston on kohteen luonteen huomioon ottaen noudatettava.	A1, D4
1.4.1.5. Korkea taso	*Ennen sopimuksen solmimista organisaatio auditoi tai pyytää kirjallisen selvityksen kumppanin yhteistyön kohteeseen liittyvistä tietoturvamenettelyistä.*	D4
1.4.1.6. Korkea taso	*Sopimuksessa on määritelty sanktiot tietoturvapoikkeamista ja - loukkauksista.*	D4
1.4.2 Toiminnan varmistaminen erityistilanteessa		
1.4.2.1. Perustaso	Tietoturvallisuuden valvonta sekä poikkeamien kirjaaminen ja raportointi on organisoitu ja vastuutettu yhteistyön kohteeseen liittyen.	D4
1.4.2.2. Perustaso	Havaituista kumppania koskevista tietoturvapoikkeamista tiedotetaan kumppanille välittömästi ja poikkeaman korjaustoimet aloitetaan sovitusti.	D4

1.4.2.3. Korot. taso	Tietoturvapoikkeaman käsittelystä yhteistyössä on kirjalliset ohjeet.	D4
1.4.2.4. Korot. taso	Poikkeamasta ja sen syystä valmistuu kirjallinen raportti	C1, D4, F
1.4.2.5. Korot. taso	Organisaatiokohtaisia jatkuvuusharjoituksia toteutetaan säännöllisesti	C1, F
1.4.2.6. Korkea taso	*Yhteistoimintaa erityistilanteessa harjoitellaan kumppanin kanssa.*	C1, D4, F
1.4.2.7. Korkea taso	*Tietoa poikkeamien syistä käytetään sopimusten ja toiminnan parantamiseen.*	C1, D4, F
1.5 Prosessit		
1.5.1 Tietoaineistojen hallinta		
1.5.1.1. Suomen erityisv.	Organisaatiolla on arkistonmuodostussuunnitelma (Arkistolaki 8§), josta käytetään usein myös nimitystä tiedonhallinta- tai tiedonohjaussuunnitelma.	A1, B4
1.5.1.2. Suomen erityisv.	Organisaatio pitää luetteloa organisaatioon käsiteltäviksi tulleista ja käsitellyistä asioista (Julkisuuslaki 18§).	A1, B4
1.5.1.3. Perustaso	Työntekijät tietävät miten tietoaineistoja organisaatiossa käsitellään.	D6
1.5.1.4. Perustaso	Organisaation tuottamasta kirjallisesta asiakirjasta käy ilmi kuka sen on laatinut ja milloin sekä sen hyväksymisen tila.	D5
1.5.1.5. Perustaso	Hävitettäväksi tarkoitettavat asiakirjat on tuhottava niin, että luottamuksellisuus ja tietosuoja on varmistettu.	D6
1.5.1.6. Korot. taso	Organisaatiossa on tietoaineistojen käsittelyn kirjallinen ohje, jossa kerrotaan, miten asiakirjat hyväksytään, katselmoidaan ja mikä organisaation aineisto on salassa pidettävää tai muun vaitiolovelvollisuuden alaista	D6
1.5.1.7. Korkea taso	*Organisaatiossa käytössä olevat tietoaineistojen hallinnan välineet tukevat aineistojen luokittelua ja arkistointia.*	B3, B4
1.6 Toiminnan arvioinnille ja todentamiselle asetettavat vaatimukset		
1.6.1 Toiminnan arviointi ja todentaminen		
1.6.1.1. Perustaso	Organisaatiossa tehdään säännöllisesti tietoturvallisuuden auditointeja tai arviointeja.	D3, F
1.6.1.2. Perustaso	Auditoinnit tai arvioinnit ovat suunniteltuja ja johdon hyväksymiä.	D3
1.6.1.3. Perustaso	Auditoinnin tai arvioinnin tulokset raportoidaan toiminnon tai kohteen omistajalle.	D3
1.6.1.4. Perustaso	Auditointien tai arviointien suosituksista pidetään koko organisaation tasolla kirjaa ja parannustoimenpiteiden toteutumista seurataan.	D3
1.6.1.5. Korot. taso	Tietoturva-auditointeja tai arviointeja tehdään joka vuosi.	D3, F
1.6.1.6. Korot. taso	Organisaatiossa on kirjallinen johdon hyväksymä auditointi- tai arviointiprosessi, jossa on mm. määritelty auditoijien tai arvioijien pätevyysvaatimukset.	D3
1.6.1.7. Korot. taso	Raportin pohjalta toiminnon tai kohteen omistaja määrittelee ja vastuuttaa parannustoimenpiteet, joilla havaitut riskit saadaan hyväksyttävälle tasolle.	C1, D1
1.6.1.8. Korkea taso	*Auditoinnit tai arvioinnit käyvät läpi organisaation*	D3

	avaintoiminnot 5 vuoden aikajaksolla.	
1.6.1.9. Korkea taso	*Tietoturva-auditoinneissa tai arvioinneissa käytetään myös ulkopuolisia resursseja.*	D3
2 Tietojärjestelmien hallinnan vaatimukset		
2.1. Raportointi tietoturvavastaavalle		
2.1.1. Perustaso	Säännöllinen raportointi IT-järjestelmien ja niiden hallinnan tietoturvallisuuden tilasta tietoturvavastaavalle on organisoitu ja vastuutettu.	D1, D4
2.1.2. Perustaso	Vakavista tietoturvatapahtumista kerrotaan tietoturvavastaavalle viivytyksettä.	D4, D6
2.1.3 Korot. taso	Raportointi on kirjallinen.	B3, D4
2.1.4. Korkea taso	Raportointi perustuu sovittuihin tietoturvatavoitteisiin ja niiden mittareihin.	B3, D3
2.2. Omaisuuden hallinta		
2.2.1. Suomen erityisv.	Organisaation omistamista henkilörekistereistä on Henkilötietolain 10§ mukainen rekisteriseloste ja se on asetettu rekisteröityjen nähtäville.	B3, B4
2.2.2. Suomen erityisv.	Kustakin tietojärjestelmästä on Julkisuuslain 18§ mukainen tietojärjestelmäkuvaus.	B3, B4
2.2.3. Perustaso	Organisaatiossa on luettelot organisaation omistamista ja käyttämistä fyysisistä tai virtuaalisista laitteista, tietojärjestelmistä, palveluista sekä ohjelmistoista ja lisensseistä.	B3
2.2.4. Perustaso	Laitteiden, rekistereiden ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu.	B3
2.2.5. Perustaso	Laite-, tietojärjestelmä-, palvelu- ja ohjelmistoluettelojen sekä lain mukaisten selosteiden ja kuvausten päivitys on organisoitu ja vastuutettu.	B3
2.2.6. Korot. taso	Omistaja on dokumentoinut laitteiden, tietojärjestelmien ja rekistereiden tietosisällön.	B3
2.2.7. Korot. taso	Omistaja on luokitellut omaisuuden tarvittavan tietoturvallisuustason mukaisesti.	B2, B3
2.2.8. Korot. taso	Omistajat katselmoivat laite-, rekisteri-, palvelu- ja ohjelmistoluetteloiden sekä lain mukaisten selosteiden ja kuvausten sisällön säännöllisesti.	B2, B3, D3
2.3 Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto		
2.3.1. Perustaso	Tietojärjestelmän ja työasemien käyttöönottoasennuksessa ja käytöstä poistamisessa otetaan huomioon järjestelmän tietosisällön tietoturvavaatimukset.	B3, E
2.3.2. Perustaso	Tietojärjestelmien ja työasemien käyttöönottoon ja käytöstä poistamiseen liittyvät toimenpiteet on vastuutettu ja organisoitu.	B3, E
2.3.3. Korot. taso	Tietojärjestelmien ja työasemien ensiasennuksesta ja käytöstä poistosta on kirjallinen ohjeisto, jossa kerrotaan mm. eri turvatasoilla käytettävät tietoturvaasetukset sekä laitteiden käsittelyn ja massamuistien tyhjennyksen menettelyt silloin kun ne siirtyvät ympäristöstä toiseen tai kun ne poistuvat organisaation hallinnasta.	B3, E
2.3.4. Korot. taso	Ohjeiden päivitys on vastuutettu ja organisoitu.	B3, D5
2.3.5. Korkea taso	Korkean tietoturvallisuustason tietojärjestelmät ja työ-	B3, E

	asemat kovennetaan.	
2.3.6. Korkea taso	Tietojärjestelmät ja työasemat huolletaan niin, että massamuisteilla olevat tiedot eivät joudu ulkopuolisten haltuun.	B3, E
2.4 Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta		
2.4.1. Perustaso	Laitteiden ja tietojärjestelmien päivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus on vastuutettu ja organisoitu erityisesti tietoturvapäivitysten osalta.	B3, E
2.4.2. Perustaso	Laitteiden ja tietojärjestelmien muutostarpeen seuranta, muutospäätösten teko ja muutosten toteutus on vastuutettu ja organisoitu.	B3, E
2.4.3. Perustaso	Organisaatiolla on periaatteet, jotka kertovat, millaiset päivitykset tai muutokset asennetaan välittömästi ja millaisiin päivityksiin ja muutoksiin käytetään riskitason huomioon ottavaa tarveharkintaa.	B3, E
2.4.4. Korot. taso	Muut kuin päivitys- ja muutoshallintaperiaatteiden perusteella kiireellisinä toteutettavat päivitykset tai muutokset tehdään vain etukäteen sovittuna aikana (ns. huoltoikkuna).	B3, E
2.4.5. Korot. taso	Tietojärjestelmään saadaan asentaa tai liittää vain järjestelmän omistajan hyväksymiä ohjelmia ja laitteita.	B3, E
2.4.6. Korot. taso	Organisaation päivitys- ja muutosperiaatteet ovat kirjalliset.	B3, D5, E
2.4.7. Korkea taso	Päivitysten ajantasaisuutta ja onnistumista mitataan ja seurataan.	B3, D3
2.4.8. Korkea taso	Päivitykset ja muutokset testataan ennen kuin ne otetaan tuotantokäyttöön.	B3, E
2.4.9. Korkea taso	Organisaatiossa osallistutaan tietoturvatilanteen seuranta- tai yhteistyöryhmiin.	D3, D4
2.5 Turva-alueiden muodostus ja niiden välinen suodatus		
2.5.1. Perustaso	Organisaatiossa on tunnistettu ja eriytetty tietoverkon eri suojaustasoa vaativat osat ja eri suojaustason verkkojen välistä liikennettä rajoitetaan ja suodatetaan.	B3, E
2.5.2. Perustaso	Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden tietoliikennelaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen.	B3, E
2.5.3. Perustaso	Palomuurien tai muiden suodatuslaitteiden suodatussäännöt on dokumentoitu.	B3, E
2.5.4. Perustaso	Julkisesta verkosta organisaatioon sisäänpäin tulevaa liikennettä rajoitetaan ja suodatetaan ”kaikki liikenne on kielletty ellei erikseen sallittu” -periaatteella. Myös organisaatiosta julkiseen verkkoon lähtevää liikennettä suodatetaan.	B3, E
2.5.5. Perustaso	Organisaatiossa on etäkäyttöperiaatteet.	B3, D6, E
2.5.6. Korot. taso	Organisaatiossa on kirjallinen palomuuri- ja liikenteensuodatuspolitiikka sekä kirjallinen sääntöjen päivitysprosessi.	B3, E
2.5.7. Korot. taso	Palomuurien tai muiden suodatuslaitteiden säännöstöjen ajantasaisuutta katselmoidaan säännöllisesti.	D3
2.5.8 Korot. taso	Tietoverkkoihin saadaan liittää vain verkon omistajan hyväksymiä laitteita.	B3, E

2.5.9. Korot. taso	Etäkäyttöperiaatteet ovat kirjalliset. Periaatteissa kerrotaan minkälaisilla laitteilla ja mistä verkoista yhteyttä voidaan ottaa sekä mitä järjestelmiä käyttää ja ylläpitää.	B3, D6, E
2.5.10 Korkea taso	Tietoverkkoja valvotaan tietoturvapoikkeamien ja -loukkausten varalta ja havaittuihin poikkeamiin reagoidaan.	B3, C1, E, F
2.6 Pääsynvalvonta		
2.6.1. Perustaso	Tietojärjestelmän omistaja hyväksyy kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmän sisältämien tietojen käyttöön tarvitaan.	B3, E
2.6.2. Perustaso	Sekä onnistuneet että epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti.	B3, E
2.6.3. Perustaso	Huonolaatuisten salasanojen käyttöä estetään.	B3, E
2.6.4 Korot. taso	Organisaatiossa on kirjallinen pääsynvalvontapolitiikka, jossa kerrotaan mm. eri turvatasoilla hyväksyttävät tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset ja vaihtoperiaatteet.	B3, B5, E
2.6.5. Korot. taso	Pääsynvalvontalokit säilytetään niin, että niitä ei päästä jälkikäteen muuttamaan.	B3, E
2.6.6. Korot. taso	Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.	B3, E
2.6.7. Korkea taso	Varmenteiden myöntämisestä, käytöstä ja uusimisesta on kirjallinen ohjeisto ja käytössä olevista varmenteista ajantasainen lista.	B3, E
2.6.8. Korkea taso	Korkean tason järjestelmissä pääsynvalvontalokeja ja kirjausketjuja tuotetaan myös järjestelmän sisällä toimimisesta toiminnan vaatimusten mukaisesti.	B3, E
2.6.9. Korkea taso	Tunnistuksen epäonnistumista sekä muita valtuuksien puutteeseen kariutuvia toimenpideyrityksiä tilastoidaan.	B3, D3, E
2.7 Käyttäjien ja käyttövaltuuksien hallinta		
2.7.1. Perustaso	Organisaatiossa on sovittu käyttövaltuuksien hallintaperiaatteet. Tunnusten ja valtuuksien myöntö, muuttaminen ja poisto on organisoitu ja vastuutettu periaatteiden mukaisesti.	B3, B5, E
2.7.2. Perustaso	Käyttövaltuudet ovat henkilö- tai roolikohtaisia.	B3, E
2.7.3. Perustaso	Käyttövaltuudet perustuvat palvelussuhteeseen tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö estetään teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä.	B3, E
2.7.4. Perustaso	Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää.	B3, E
2.7.5. Perustaso	Uuden henkilön tullessa organisaatioon ensimmäinen tunnistus tehdään valokuvallisesta henkilöllisyystodistuksesta tai sähköiseen palveluun rekisteröitymisen osalta käyttäen samantasoista todennusmenetelmää.	B3, D6, E
2.7.6. Korot. taso	Organisaatiossa on kirjallinen käyttövaltuuspolitiikka ja hallintaprosessi.	B3, B5, E
2.7.7. Korot. taso	Jokaisella käyttövaltuudella on omistaja.	B3, E

2.7.8. Koro. taso	Järjestelmien käyttövaltuudet katselmoidaan vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja valtuudet suljetaan tai poistetaan.	B3, D3, E
2.7.9. Korot. taso	Myöntöprosessista jää jälki, millä perusteella käyttäjälle on myönnetty käyttövaltuus.	B3, E
2.7.10 Korot. taso	Kielletyt työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa kiellettyjen yhdistelmien syntymistä seurataan ja estetään.	B3, E
2.7.11. Korkea taso	Ylläpito- ja pääkäyttäjäoikeuksien määrää seurataan ja tilastoidaan.	B3, D3, E
2.7.12. Korkea taso	Käyttövaltuuksien poistoon kuluvaa aikaa seurataan ja tilastoidaan.	B3, D3, E
2.7.13. Korkea taso	Organisaatiossa on dokumentoitu menettely käyttäjätunnuksen tai käyttövaltuuksien välittömään poistoon tai passivointiin.	B3, E
2.8.1. Perustaso	Organisaatiossa suodatetaan haittaohjelmia sekä työasematasolla että kaikissa sähköpostin ja www-liikenteen sisääntulo- ja ulosmenopisteissä.	B3, E
2.8.2. Perustaso	Haittaohjelmakuvaukset päivittyvät säännöllisesti ja automaattisesti.	B3, E
2.8.3. Korot. taso	Käyttäjiä on ohjeistettu, miten haittaohjelmia levittäviä sähköposteja voidaan yrittää tunnistaa ja mitä tehdä haittaohjelmaepäilytilanteessa.	B3, D6
2.8.4. Korot. taso	Haittaohjelmistokuvausten ajantasaisuutta valvotaan.	B3, E
2.8.5. Korkea taso	Työasema ei saa kytkeytyä korkean tietoturvallisuustason verkkoihin, ellei ole varmistettu että se on puhdas haittaohjelmista.	B3, B5, E
2.8.6. Korkea taso	Haittaohjelmasuodatuksen kattavuutta mitataan ja seurataan.	B3, D3
2.9. Fyysisen ympäristön suojaus		
2.9.1. Perustaso	Organisaatiossa on tunnistettu omien tilojen tarvitsema suojausluokka ja eriytetty eri suojausluokkaa vaativat osat rajoittamalla kulkua tilojen välillä.	B2, B3, E
2.9.2. Perustaso	Organisaatiossa on sovittu henkilö- tai roolitasolla, kenellä on pääsy IT-laitetiloihin ja kulunvalvonta on organisoitu tämän mukaisesti.	B3, E
2.9.3. Korot. taso	Tilojen eriytys eri suojausluokkiin on dokumentoitu.	B3, E
2.9.4. Korot. taso	Tietoliikennelaitteiden, -yhteyksien ja kytkentäpisteiden sijainti on otettu huomioon suojausluokittelussa.	B2, B3, E
2.9.5. Korkea taso	Tiloja ja niissä kulkua valvotaan automaattisesti ja valvontamenettely on dokumentoitu.	B3, D6, E
2.9.6. Korkea taso	Ulkopuolisten toimintaa IT-laitetiloissa valvotaan.	B3, D6, E
2.10. Varmuuskopiointi		
2.10.1. Perustaso	Organisaatiossa on vastuutettu ja organisoitu varmuuskopioiden ottaminen.	B3, D1, C1, E, F
2.10.2. Perustaso	Organisaatiossa on tunnistettu varmuuskopioinnin kannalta olennaiset suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti. Myös varmuuskopioiden palauttaminen on suunniteltu.	B2, B3, C1, E, F
2.10.3. Korot. taso	Organisaatiossa on kirjallinen varmuuskopiointipolitiikka ja -prosessi, jotka on muodostettu ottaen huomioon toiminnan vaatimukset ja joissa ohjeistetaan varmuus- ja suojakopioiden käsittely siirron ja varastoinnin aikana.	B3, B5, C1, E, F

2.10.4. Korot. taso	Organisaatiossa otetaan tärkeimmistä järjestelmistä suojakopioita, joita säilytetään eri palotilassa kun varsinaisia varmuuskopioita.	B3, C1, E, F
2.10.5. Korkea taso	Eri järjestelmien varmuuskopioiden palautusta testataan säännöllisesti.	B3, C1, E, F
2.10.6. Korkea taso	Varmuuskopioilta palautettavien tietojen määrää ja palautuksen syitä tilastoidaan.	B3, D3, E, F
2.11 Tietoturvapoikkeamien valvonta		
2.11.1. Suomen erityisv.	Sähköisten viestien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös lokitietojen käsittelyssä (Sähköisen viestinnän tietosuojalaki 4§ ja 5§).	B3, B4, E
2.11.2. Perustaso	Laitteet, ohjelmistot sekä tietojärjestelmät tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan.	B3, D3, E
2.11.3. Korot. taso	Organisaatiossa on kirjallinen lokienkeräys-, hälytys- ja seurantapolitiikka, joka on muodostettu ottaen huomioon toiminnan vaatimukset.	B3, B5, E
2.11.4. Korkea taso	Lokien seurannan perusteella muodostetaan tilannekuvaa ja havaitaan tietoturvapoikkeamia sekä kehitetään toimintaa.	B3, C1, D3, E
2.12 Tietojärjestelmien toipuminen häiriöistä		
2.12.1. Suomen erityisv.	ICT-järjestelmien omistajat tietävät ICT-varautumiseen liittyvät vastuunsa ja toiminta on organisoitu ja vastuutettu sen mukaisesti.	B3, B4, C1, D1, E
2.12.2. Perustaso	ICT-järjestelmien häiriöiden selvitys ja niistä toipuminen on organisoitu ja vastuutettu.	B3, C1, D1, E
2.12.3. Perustaso	Organisaatiossa on yleinen toipumisstrategia ja suunnitelma tärkeimpien omien järjestelmien häiriöille, jossa on mm. johdon hyväksymä tärkeysjärjestys ICT-palveluille.	B3, C1, E
2.12.4. Korot. taso	Organisaatiolla on tärkeimmistä järjestelmistä kirjalliset toipumissuunnitelmat.	B3, C1, E
2.12.5. Korkea taso	Järjestelmien häiriöistä ja niiden syistä pidetään kirjaa. Tietoa käytetään hyväksi riskianalyyseissä ja palvelutasosopimusten teossa.	B3, D3, E
2.13 Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta		
2.13.1. Perustaso	Järjestelmän omistaja hyväksyy, mitä tietoturvallisuustasoa järjestelmän tulee valmiina tai muutosten jälkeen noudattaa.	B3, E
2.13.2. Perustaso	Järjestelmään kohdistetaan riskianalyysi, jolla pyritään löytämään tietoturvavaatimukset tarjouspyyntöön, vaatimusmäärittelyyn tai uuden version asennuksen projektisuunnitelmaan.	B3, C2, D4
2.13.3. Perustaso	Hankkivalla organisaatiolla on tietoturvavaatimuksia sisältävä tietojärjestelmien arkkitehtuurilinjaus, jonka mukaisia hankittavien tai kehitettävien järjestelmien tulee olla.	B3, D4, E
2.13.4. Korot. taso	Järjestelmän toimivuus testataan ennen tuotantokäyttöön ottamista.	B3, E, F
2.13.5. Korot. taso	Jos organisaatio hankkii räätälöityjä tietojärjestelmiä tai kehittää niitä itse, organisaatiolla on dokumentoitu tietojärjestelmän kehitysprosessi, jonka eri vaiheissa on	B3, D4, E

	otettu tietoturvallisuus huomioon.	
2.13.6. Korot. taso	Osana hankinta- tai kehitysprojektia järjestelmästä valmistuu kirjallinen turvallisuussuunnitelma ja käyttäjän ohje, joissa kerrotaan miten järjestelmä suojataan tuotantokäytössä ja millaiset ovat käyttäjiltä vaadittavat tietoturvatoimenpiteet.	B3, E
2.13.7. Korot. taso	Järjestelmän määritykset ja toteutukset on auditoitu tietoturvallisuuden osalta	B3, D3, E
2.13.8. Korkea taso	Tietoturvavastaava tarkastaa järjestelmän tietoturvakuvauksen, -suunnitelman tai -suunnitelmat.	B3, D3
2.13.9. Korkea taso	Kehitys- tai räätälöintityön aikana järjestetään katselmointeja tietoturvallisuuden kannalta kriittisiin osiin ja katselmoinneista valmistuu pöytäkirja.	B3, D3

Taulukko 1.1. Projektioppaan vaiheiden liittyminen VAHTI 2/2010 tietoturvatasovaatimuksiin.

Liite 2 Oppaan tehtävien liittyminen KATAKRIin

Alla taulukossa 2 oppaan tehtävät on rinnastettu KATAKRI:n kriteereihin. Kustakin kriteeristä on kuvattu tulkinta (“otsikko”) sen pääasiallisesta sisällöstä. KATAKRI löytyy web-osoitteesta http://www.defmin.fi/files/1525/Katakri.pdf .

Tunnus		**Kriteerin pääasiallinen sisältö**	Tehtävä
A	**101**	Johdon tukema ja tarkistama turvallisuuspolitiikka	B5, D7
A	**102**	Turvallisuuspolitiikan ja/tai turvallisuuden johtamisen riittävän kattavuuden varmistaminen turvallisuusdokumentaatiossa	A2, B1, B3, B4, C5, D2
A	**103**	Turvallisuusdokumentaation vastaavuus organisaation riskeihin nähden	B3, B5, C1, C2, C3, C4, D1, D2, D3, D5, D6, D7, D8
A	**104**	Toimiminen turvallisuuspolitiikan mukaisesti	A3, B4, B5, D1, D2, D3, D5, D6, D7, D8
A	**105**	Lainsäädännön ja paikallisten turvallisuusmääräysten huomioiminen turvallisuuspolitiikassa	A3, B4, B5, D7
A	**106**	Turvallisuuspolitiikasta tiedottaminen	D5, D6, D7
A	**107**	Turvallisuuspolitiikan ohjaavuus jatkuvaan parantamiseen	B5, D7,F
A	**108**	Keskeisten turvallisuustavoitteiden ilmaiseminen turvallisuuspolitiikassa	A1, B4, C5, D2
A	**201**	Dokumentoitu ohjelma tietoturvallisuuden johtamisen ja turvallisuustyön tavoitteiden varmistamiseksi	D8, F
A	**202**	Menetelmien, vastuiden ja aikataulujen erittely toimintaohjelmassa	D8, F
A	**203**	Toimintaohjelman säännöllinen tarkistaminen	F
A	**301**	Turvallisuustyön tavoitteiden asettaminen liiketoiminnan ja turvallisuuspolitiikan mukaisesti	A1, B4, C5, D2
A	**302**	Turvallisuustavoitteiden asettaminen eri hierarkiatasoille ja toiminnoille	A1, B3

A	**303**	Tavoitteiden mitattavuuden varmistaminen	A1, D3
A	**304**	Tavoitteiden aikataulutus	A1
A	**305**	Tavoitteiden asettaminen vaatimukset, mahdollisuudet ja rajoitukset huomioiden	A1
A	**401**	Menetelmä turvallisuusriskien tunnistamiseen ja arviointiin	C1
A	**402**	Riskienarvioinnin riittävä kattavuus (normaalioiminta, erityistilanteet, onnettomuudet ja hätätapaukset)	A2,B1,C1
A	**403**	Riskienarvioinnin tulosten dokumentointi ja päivittäminen	C2
A	**404**	Riskienarvioinnin huomiointi turvallisuustoiminnan tavoitteiden asettamisessa	A1, C1, C2
A	**405**	Riskienarvioinnin tulosten perusteella tehtävä priorisointi	A1, A4, C1, C2
A	**406**	Riskienarvioinnin käyttö turvallisuuskoulutuksen suunnittelussa	C2, D6
A	**407**	Riskienhallintatoimenpiteiden toteutumisen ja tehokkuuden ja valvonta	C3, D3
A	**501**	Turvallisuustyön vastuiden ja organisoinnin riittävän kattavuuden varmistaminen	A2, A3, B1, D1, D2
A	**502**	Turvallisuuden organisoinnista tiedottaminen tarvittaville osapuolille	D4, D5
A	**503**	Turvallisuustyön riittävän resursoinnin varmistaminen	D2
A	**504**	Turvallisuudesta vastaava henkilö ja turvallisuustyön kattavuus	A2, A3, B1, D1, D2
A	**505**	Turvallisuustyöstä vastaavan vastuun ja valtuuden riittävyys	A3, D1, D2
A	**506**	Johdon sitoutuminen turvallisuustavoitteisiin ja niiden saavuttamiseen sekä turvallisuuden jatkuvaan parantamiseen	A1, A5, F, B5, D7
A	**601**	Jatkuvuudenhallintamenettely	C1, F
A	**602**	Onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelyn organisointi	C1, F
A	**603**	Vastuut kriisitilanteiden, onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien vaikutusten ennalta pienentämiseksi.	A3, C1, D1, F
A	**604**	Menetelmät turvallisuuspoikkeamien havaitsemiseksi ja suojaavien että korjaavien toimenpiteiden tekemiseksi	C1, F
A	**605**	Toimenpiteiden tehokkuuden varmistaminen	D3
A	**606**	Kontrolleihin tehtävien muutosten negatiivisten vaikutusten arviointi	C3, D3
A	**607**	Turvallisuustoimenpiteiden vaikutusten analysointi.	C3, D3
A	**701**	Toimintajärjestelmä dokumentointiin	D5
A	**702**	Turvallisuustavoitteiden saavuttamisen rekisteröinti	A1, D3, D5
A	**703**	Turvallisuuskoulutusten rekisteröinti	D5, D6
A	**704**	Turvallisuuskoulutuksen riittävän tason varmistaminen	D6
A	**801**	Turvallisuusvaatimusten tärkeydestä ja oikeista toimintatavoista kouluttaminen	A1,D6
A	**802**	Henkilöstön oman työhön liittyvien turvallisuusriskien tunnistaminen	C1, D6
A	**803**	Henkilöstön riittävän osaamisen varmistaminen eri tilanteissa, joissa turvallisuus on vaarantunut	C1, D6
A	**804**	Tasovaatimukset turvallisuuskoulutukselle	D6
A	**805**	Työntekijöiden sopivuuden ja valmiuksien varmistaminen työtehtäviin	D6

A	**901**	Turvallisuudesta vastaavan henkilön raportointisuhde ylimpään johtoon	A3,D4
A	**902**	Johdon suorittama turvallisuusjärjestelmän toimivuuden säännöllinen tarkastaminen	D4, F
A	**903**	Johdon tekemä turvallisuusjärjestelmän soveltuvuuden, resurssien riittävyyden ja toiminnan tehokkuuden arviointi	D3, F
A	**904**	Seurantatarkastusten dokumentointi	D3, D5
A	**905**	Seurantatarkastusten tulosten käyttö jatkuvaan parantamiseen	D3, F
P	**101**	Luettelo hankkeeseen osallistuvista henkilöistä	D6
P	**102**	Menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi ja yhteyshenkilön yhteystietojen ajantasaisuus	A3,D6
P	**103**	Koulutusdokumentaatio saadusta koulutuksesta (hankkeeseen osallistuvat)	D4, D6
P	**104**	Vierailijaluettelon ylläpito	D4
P	**105**	Vaatimusten noudattaminen suojaustason ja turvallisuusluokituksen mukaisesti	A1, B4, D3, D6
P	**201**	Työntekijän osaamisen todentaminen keskeisten dokumenttien avulla	D5, D6
P	**202**	Työhaastattelussa saatujen tietojen oikeellisuuden varmistaminen	D5, D6
P	**203**	Työnhakijan osaamisen varmentaminen asiantuntevilla kysymyksillä	D6
P	**301**	Yrityksen arvojen mukaiseen toimintaan sitoutumisen varmistaminen työhaastattelutilanteessa	D6
P	**302**	Huumausainetestauksen käytön arviointi ja käyttömahdollisuus	D6
P	**303**	Luotettavuuden varmistaminen erityistä luotettavuutta vaativissa tehtävissä	D4, D6
P	**401**	Salassapito- ja vaitiolositoumusmenettely	D4, D6
P	**402**	Koeaikamenettely	D4, D6
P	**403**	Vastuuhenkilötietojen ja yrityskytkentöjen selvittäminen	D4, D6
P	**404**	Suppean turvallisuusselvityksen tekeminen	D4, D6
P	**405**	Perusmuotoisen turvallisuusselvityksen hakumahdollisuuden selvittäminen projektin tai tehtävän osalta	D4, D6
P	**406**	Henkilöiden luottotietojen hakeminen	D4, D6
P	**501**	Työntekijän tehtävistä, vastuista, oikeuksista sekä velvollisuuksista sopiminen tietojen suojaamisessa	D4, D6
P	**502**	Työntekijän perehdyttäminen yhtiön turvallisuusmääräyksiin	D4, D6
P	**503**	Uuden henkilön perehdyttäminen tehtäviin ja yrityksen toimintaan	D4, D6
P	**504**	Tietoturvakoulutuksen järjestäminen	D4, D6
P	**505**	Prosessikuvaukset valtuuttamisesta ja pääsyoikeuksien antamisesta tietoon ja tiloihin	B3, D4, D6
P	**601**	Sijaisuusjärjestelyihin ja avainhenkilöihin liittyvien ohjeistusten järjestäminen	D4, D6
P	**602**	Työtyytyväisyydestä ja työmotivaation ylläpidosta huolehtiminen	D4, D6
P	**603**	Työssä jaksamisen ja työkyvyn seurannan järjestäminen	D4, D6
P	**604**	Toimiminen ja vastuut työntekijän käyttäytymisen muuttuessa	D4, D6
P	**605**	Menettelyohje työsuhteen päättämisestä	D4, D6
P	**606**	Vierailukäytäntö	D4, D6
F	**101**	Suojautuminen elektronista tiedustelua vastaan pysäköintijärjeste-	B3, E

		lyjen avulla	
F	**102**	Suojautuminen elektronista tiedustelua vastaan lastaus- ja purku-alueella	B3, E
F	**103**	Kiinteistön alueella tapahtuvan liikkumisen rajoittaminen	B3, E
F	**104**	Alueen videovalvonta	B3, E
F	**201**	Kuoren rakennemateriaalit	B3, E
F	**202**	Ikkunoiden sijainti maantasoon nähden	B3, E
F	**203**	Kattoikkunoiden suojaus	B3, E
F	**204**	Kuoren aukkojen suojaaminen	B3, E
F	**205**	Ovien murtosuojaus	B3, E
F	**206**	Suurten ovien suojaus	B3, E
F	**207**	Tilojen äänieristys	B3, E
F	**208**	Kassakaapit ja holvit	B3, E
F	**209**	Tilojen pääsyoikeuksien hallinta	B3, E
F	**210**	Tilojen lukitus	B3, E
F	**211**	Mekaanisten avainten hallinnan järjestäminen	B3, E
F	**212**	Suojattavien tilojen pääsyrajoitukset	B3, E
F	**213**	Yleisavaimen pääsyrajoitukset	B3, E
F	**214**	Vartiointi- ja kiinteistönhoitohenkilöstön avaintenhallinta	B3, E
F	**215**	Huoltotoimenpiteiden järjestäminen	B3, E
F	**301**	Rikosilmoitinjärjestelmä	B3, E
F	**302**	Kulunvalvontajärjestelmä	B3, E
F	**303**	Kameravalvontajärjestelmä	B3, E
F	**304**	Palvelintilan kameravalvontajärjestelmä	B3, E
F	**305**	Rikosilmoitinjärjestelmän toimintavarmuuden testaus	B3, E
F	**306**	Kulunvalvontajärjestelmän hallinnointi	B3, E
F	**307**	Rikosilmoitinjärjestelmän hallinnointi	B3, E
F	**308**	LVI-automaation hallinta	B3, E
I	**101**	Johdon tuki organisaation tietoturvallisuudelle	A5, B5, D7F
I	**102**	Dokumentoitu ohjelma tietoturvallisuuden johtamisen ja turvallisuustyön tavoitteiden varmistamiseksi	D8, F
I	**103**	Suojattavien kohteiden tunnistaminen	B2
I	**104**	Suojattaviin kohteisiin liittyvien riskien arviointi (vrt. A104)	C1, C2
I	**105**	Organisaation tietoturvallisuuden arviointi	C1, D3
I	**106**	Tietoturvallisuus alihankinta- ym. yhteistyökuvioissa	B1, D4
I	**107**	Toimiminen tietoturvapoikkeamatilanteissa	C1, D4
I	**108**	Lakisääteisten vaatimusten huomioiminen	A1, B4
I	**109**	Menettely merkittävien tietojenkäsittely-ympäristön muutosten hallintaan	E, F
I	**201**	Hyvän tiedonhallintatavan varmistaminen käyttäjien pääsy- ja käyttöoikeuksien hallintaan	B5, E
I	**202**	Salassapito- tai vaitiolositoumusten laatiminen organisaation tietojen suojaamistarpeiden mukaisesti	D4, D6
I	**203**	Avainhenkilöriippuvuuden tunnistaminen	A3, D4, D6

I	**204**	Riittävän ohjeistuksen, koulutuksen ja tiedotuksen varmistaminen	D6
I	**205**	Hyväksyttävän käytön säännöt ja niistä tiedottaminen	D6
I	**206**	Tietoturvaohjeiden noudattamisen valvonta se seuraukset tietoturvarikkomuksista	D6
I	**207**	Ulkopuolisten työntekijöiden ja vierailijoiden tunnistaminen	D4, D6
I	**301**	Suojattavaa tietoa sisältävän tilan turvallisuus	B3, E
I	**302**	Huoltotoimenpiteiden järjestäminen valvotusti	B3, E
I	**303**	Salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin varautuminen	B3, E
I	**304**	LVIS-järjestelmien kapasiteetti ja turvallisuus	B3, E
I	**305**	Näyttöpäätenäkymän suojaaminen	B3, E
I	**401**	Tietoliikenneverkon rakenteen turvallisuus	B3, E
I	**402**	Palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöjen laatu	B3, E
I	**403**	Liikennettä suodattavien tai valvovien järjestelmien oikean toiminnan varmistaminen	B3, E
I	**404**	Hallintayhteyksien suojaus	B3, E
I	**405**	Verkon aktiivilaitteiden koventaminen	B3, E
I	**406**	Langattomien verkkojen perussuojaus	B3, E
I	**407**	Sisäverkon rakenteen näkymisen estäminen Internetiin	B3, E
I	**408**	Verkon, järjestelmien ja niiden käytön valvonta	B3, E
I	**501**	Käyttäjien tunnistaminen ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin	B3, E
I	**502**	Menettelytapa uusien järjestelmien turvalliseen asentamiseen	B3, E
I	**503**	Suojautuminen haittaohjelmia vastaan	B3, E
I	**504**	Lokimenettelyjen turvallinen toteuttaminen	B3, E
I	**505**	Salassa pidettävien tietojen turvallinen säilyttäminen tietojärjestelmissä	B3, E
I	**506**	Liikuteltavien tietovälineiden suojaaminen luvatonta pääsyä vastaan	B3, E
I	**507**	Salassa pidettävien tietojen suojaaminen huoltotoimenpiteiden ja käytöstäpoiston yhteydessä	B3, E
I	**508**	Verkon luvattomien laitteiden ja järjestelmien estäminen	B3, E
I	**509**	Salausratkaisujen riittävän turvallisuuden varmistaminen	B3, E
I	**510**	Salausavainten hallinta	B3, E
I	**511**	Istunnonhallinnan turvallinen toteuttaminen	B3, E
I	**512**	Autentikaatiodatan suojaaminen tietojärjestelmissä	B3, E
I	**513**	Ajettavan koodin turvallisuuden varmistaminen	B3, E
I	**601**	Tiedon luokittelumenettely	B2, E
I	**602**	Salassa pidettävien manuaalisten tai siirrettävillä tietovälineillä olevien tietojen turvallinen säilyttäminen	E
I	**603**	Luottamuksellisten tietojen turvallinen hävittäminen	D6
I	**604**	Salassa pidettävän tietoaineiston turvallinen kopiointi ja tulostus	D6
I	**605**	Salassa pidettävän aineiston turvallinen sähköinen välitys	D6
I	**606**	Salassa pidettävän aineiston turvallinen välitys postilla ja/tai kuriirilla	D6
I	**607**	Salassa pidettävien aineistojen välityksen seuranta	D6

I	**701**	Jatkuvuuden varmistavat suunnitelmat	C1
I	**702**	Toipumisen varmistaminen organisaation dokumentaation avulla	C1, D5
I	**703**	Ohjelmistojen, tietoliikenneyhteyksien ja ohjeislaitteiden asentamiseen liittyvät periaatteet	B5
I	**704**	Periaatteet ja mekanismit etä- ja matkatöiden riskien hallitsemiseksi	B5
I	**705**	Kehitys-/testaus- ja tuotantojärjestelmien erottaminen	E
I	**706**	Tunnettujen haavoittuvuuksien estäminen verkoissa ja sen palveluissa	E
I	**707**	Laitteiden suojaus työskentelytauoilla	D6
I	**708**	Puhtaan pöydän ja näytön politiikka	B5
I	**709**	Vaarallisten työyhdistelmien välttäminen	B5, D6
I	**710**	Riittävästä varmuuskopioinnista huolehtiminen	C1

Taulukko 2.1 Projektimallin osien liittyminen KATAKRIin.

Liite 3 Oppaan liittyminen asetukseen tietoturvallisuudesta valtionhallinnossa

Alla on esitetty yhteenveto asetuksesta tietoturvallisuudesta valtionhallinnossa. Tekstissä on suluissa merkitty ne oppaan tehtävät, jotka liittyvät ko. asetuksessa esitettyyn asiaan.

Asetuksen sisältö

Asetus tietoturvallisuudesta valtionhallinnossa (TTA 681/2010, ”tietoturvallisuusasetus”) astui voimaan 1.10.2010. Se annettiin Lain viranomaisen toiminnan julkisuudesta (JulL 621/1999, ”julkisuuslaki”) nojalla.

Asetus toi valtionhallintoon yhteisen asiakirjaluokittelun, velvoitteen saavuttaa tietoturvallisuuden perustaso 1.10.2013 mennessä ja velvoitteen tietoturvallisuuden korotetun tai korkean tason saavuttamiseksi sille osalle valtionhallintoa, joka käsittelee usein suojaustason III tai sitä korkeamman suojaustason tietoa. Asetus ei suoraan kerro, missä korotetun ja korkean tason vaatimukset on kuvattu. Valtiovarainministeriön VAHTI – työryhmä on laatinut asetusta tukevan ohjeen nimeltä ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta” (VAHTI 2/2010). Ohjeen liitteessä 5 on kuvattu vaatimukset eri tietoturvatasoille. Tietoturvatasovaatimuksia on kuvattu myös KATAKRI:ssa (Kansallinen turvallisuusauditointikriteeristö).

Tietoturvallisuuden suunnittelun perusteet

Tietoturvallisuusasetus 4, 5§ 1 mom. 1k ja julkisuuslaki 18§ 1 mom. 4k velvoittavat toteuttamaan suojaustoimet suojaustarpeen mukaisesti. (Ks. tehtävien **B2** ja **B3** tiedonkeruutaulukot) Suojaustarpeiden arviointi tulee perustua riskien tunnistamiseen ja sopivien suojamenettelyiden arviointiin (ks. **B2** ja **B3** tiedonkeruutaulukot). Arvioinnissa huomioidaan käytettävissä olevat keinot, kustannukset ja toimenpiteillä saatavat vaikutukset.

Velvoite tietoturvallisuuden perustason saavuttamisesta

Tietoturvallisuuden perustaso on kuvattu asetuksen 2 luvun 5§:ssä. ”Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että:

1) viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan (ks. **C1** ja **C2**);

2) viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään (ks. **D1**, **D2** ja **D6**);

3) asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään (ks. **D1**,**D5** ja **D6**);

4) tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi (ks. **C1**, **C2**);

5) asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi (ks. **B5**, **E**);

6) tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä (**E**);

7) asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja (**E**);

8) henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla (**D6**);

9) henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä (**D6**);

10) annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti (**D6**).

Valtionhallinnon viranomaisen velvollisuudesta huolehtia tietojen suojaamisesta annettaessa salassa pidettäviä tietoja toimeksiantotehtävän suorittamista varten säädetään viranomaisten toiminnan julkisuudesta annetun lain 26 §:n 2 momentissa. Henkilörekisteriin talletettujen henkilötietojen antamisesta säädetään lisäksi henkilötietolain 32 §:n 2 momentissa.” (ks. **B4** vaatimustenmukaisuus)

Velvoite korotetun tai korkean tason saavuttamisesta

Perustason lisäksi tietoturvallisuusasetus velvoittaa tietoturvallisuuden korotetun tai korkean tason saavuttamiseen niille valtionhallinnon toimijoille, jotka käsittelevät usein suojaustason III tai sitä korkeamman suojaustason tietoja.

TTA 16§ 3 mom.:

”Valtionhallinnon viranomainen voi sallia, että suojaustasoon III kuuluva asiakirja talletetaan viranomaisen tietoverkkoon liitetylle laitteelle, jos verkon käyttö on rajoitettu ja asiakirja talletetaan salattuna tai muutoin suojattuna siten, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuustason vaatimukset. Sama koskee suojaustasoon IV kuuluvaa arkaluonteisia henkilötietoja tai biometrisiä tunnistetietoja sisältävää henkilörekisteriin talletettua asiakirjaa.”(ks. **B2**, **B3**, **B4**, **E**)

TTA 16§ 4 mom.:

”Laadittaessa suojaustasoon I–III kuuluvaa asiakirjaa sähköisessä muodossa ja sitä muokattaessa on pidettävä huolta, että hajasäteilystä aiheutuvia haittoja voidaan riittävästi vähentää. Jos laite on liitetty tietoverkkoon, tietoverkon on lisäksi täytettävä 1 momentin 2 kohdassa taikka 2 tai 3 momentissa säädetyt edellytykset.” (ks. **B2**, **B3**, **B4**, **E**)

TTA 19§ 3 mom.:

”Valtionhallinnon viranomainen voi sallia, että suojaustasoon III kuuluva asiakirja siirretään viranomaisen tietoverkossa, jonka käyttö on rajoitettu, jos viranomainen on varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuuden tason vaatimukset. Sama koskee suojaustasoon IV kuuluvien valtakunnalliseen henkilörekisteriin talletettujen arkaluonteisten henkilötietojen tai biometristen tunnistetietojen siirtämistä tietoverkossa. Suojaustasoon IV kuuluvan muun asiakirjan saa siirtää valtionhallinnon viranomaisen päättämällä tavalla.” (ks. **B2**, **B3**, **B4**, **E**)